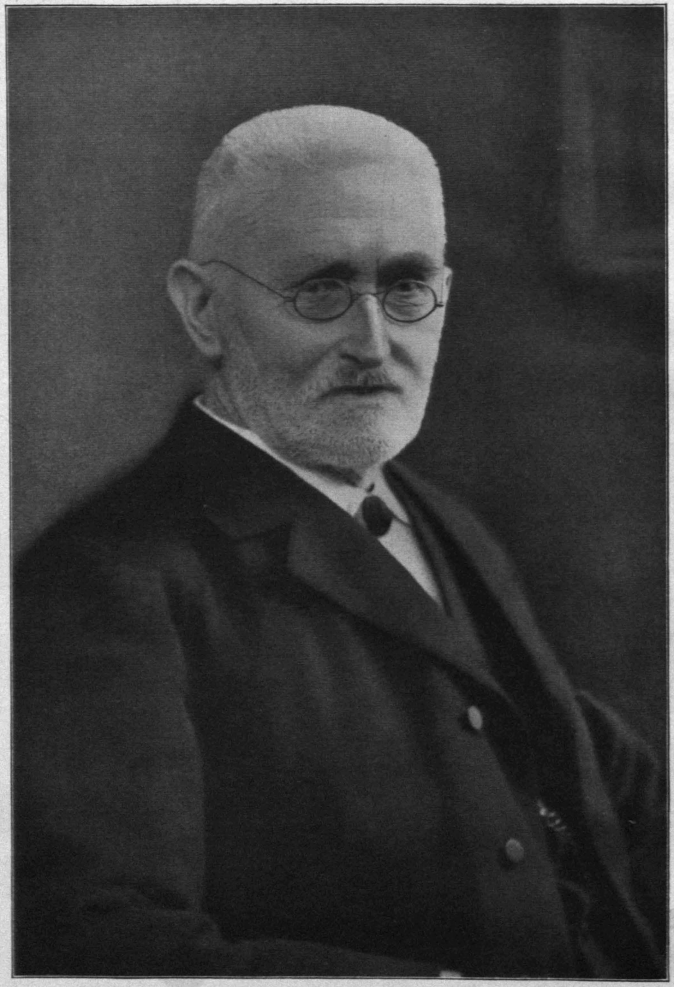


R. Dedekind.

Richard Dedekind

Gesammelte mathematische Werke

Herausgegeben von

Robert Fricke
in Braunschweig

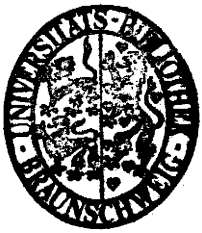
Emmy Noether
in Göttingen

Öystein Ore
in New Haven

Erster Band

Mit einem Bildnis Dedekinds

Druck und Verlag von Friedr. Vieweg & Sohn Akt.-Ges.
Braunschweig 1930



Printed in Germany

Inhaltsverzeichnis.

I.

Über die Elemente der Theorie der Eulerschen Integrale.

[Inauguraldissertation, Göttingen 1852.]

Es ist bekannt, daß die Ausführung der indirekten Operationen in der Analysis meist auf viel bedeutendere Schwierigkeiten stößt, als die der direkten; aber gerade dieser scheinbar unglückliche Umstand hat auf die Entwicklung der Mathematik stets den günstigsten Einfluß ausgeübt. Nicht nur, daß die Besiegung dieser Schwierigkeiten, wenn sie möglich, immer einen eigentümlichen Reiz für den Mathematiker darbietet, sondern auch gerade die Fälle, in welchen dies mit den früher eingeführten Begriffen und Hilfsmitteln nicht möglich war, haben immer der weiteren Ausbildung der Mathematik ganz neue Felder eröffnet; so führen z. B. die Operationen der Subtraktion, Division und Wurzelausziehung auf die Begriffe der negativen, gebrochenen und imaginären Zahlen, von denen jeder das Gebiet der Mathematik so außerordentlich erweitert hat. Ganz ähnlich verhält es sich nun auch in der höheren Analysis mit dem ihr zugrunde liegenden Begriff der Funktion, welcher sich anfangs nur auf die in der Elementarmathematik gelehrten Operationen (die ihnen entsprechenden Funktionen könnte man füglich Elementarfunktionen nennen) und auf deren Zusammensetzung stützt. Die Differentialrechnung, der mächtigste Hebel zur Entwicklung der Theorie der Funktionen, findet in ihrer Ausführung keine Schwierigkeiten, d. h. das Differentiieren der aus den Operationen der Elementarmathematik gebildeten Funktionen führt wieder auf eben solche Funktionen. Dagegen ist es der umgekehrten Rechnungsart, welche in ihrer Gesamtheit die Integralrechnung bildet, nur in verhältnismäßig wenigen Fällen gelungen, dasselbe zu leisten; in den meisten ist es bisher nicht geglückt, oder vielleicht auch ganz unmöglich, die Integrale

gegebener Funktionen mit Hilfe eben solcher darzustellen. Aber gerade dieser Umstand hat zu einer beträchtlichen Erweiterung des Begriffs der Funktion geführt, indem man solchen nicht darstellbaren Integralen neue Namen und Bezeichnungen beigelegt, und sie dadurch in den Kreis der früheren Funktionen eingeführt hat. Bei der Entwicklung der Theorie solcher Integralfunktionen sind nun namentlich die Fälle von der größten Wichtigkeit, in denen sie sich auf die bisher allein gebräuchlichen Funktionen zurückführen lassen, indem dadurch ihr Verlauf deutlicher hervortritt, und auch oft Mittel an die Hand gegeben werden, ihre Berechnung zu erleichtern. Die Zusammenstellung dieser Fälle für die Eulerschen Integrale, mit besonderer Rücksicht auf die dabei anzuwendende Methode, ist der Hauptzweck der folgenden Abhandlung.

1.

Es ist zuerst erforderlich, die Fundamentaleigenschaften der Eulerschen Integrale kurz in Erinnerung zu bringen. Die Definitionen dieser Funktionen liegen in den Gleichungen

$$(1) \qquad B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1}\,dx; \quad \Gamma(\mu) = \int_0^\infty x^{\mu-1}e^{-x}\,dx.$$

Die Integrale rechts heißen Eulersche Integrale der ersten und der zweiten Art; die ersteren lassen sich leicht auf die letzteren zurückführen. Führt man nämlich in dem Doppelintegral

$$\int_0^\infty \int_0^\infty e^{-(x+y)}x^{a-1}y^{b-1}\,dy\,dx = \Gamma(a)\,\Gamma(b)$$

für x und y zwei neue Variabeln r und w ein, indem man $x+y=r$ und $x=rw$ setzt, woraus $dy\,dx = r\,dr\,dw$ folgt, so erhält man

$$\int_0^\infty e^{-r}r^{a+b-1}\,dr \int_0^1 w^{a-1}(1-w)^{b-1}\,dw = \Gamma(a)\,\Gamma(b)$$

und daraus zufolge der Definitionen von B und Γ

$$(2) \qquad B(a,b) = \frac{\Gamma(a)\,\Gamma(b)}{\Gamma(a+b)},$$

woraus sich zugleich ergibt, daß $B(b,a) = B(a,b)$ eine symmetrische Funktion von a und b ist, was man auch direkt zeigen kann, wenn man in dem Integral B $(1-x)$ statt x setzt.

Setzt man in dem Integral Γrx statt x, und nimmt r als eine positive Konstante an, so erhält man

$$(3) \qquad \int_0^\infty x^{\mu-1} e^{-rx} \mathrm{d}x = \frac{\Gamma(\mu)}{r^\mu}$$

und hieraus durch $n$malige partielle Differentiation in bezug auf r die wichtige Relation

$$(4) \qquad \Gamma(\mu+n) = (\mu+n-1)(\mu+n-2)\ldots(\mu+1)\mu\Gamma(\mu).$$

Es leuchtet ein, daß man $\Gamma(\mu)$ nur für jedes μ innerhalb eines Intervalls zu berechnen braucht, welches eine Einheit umfaßt, um daraus mit Hilfe dieser Gleichung $\Gamma(\mu)$ für jedes andere μ zu finden.

2.

Aus den eben entwickelten Formeln lassen sich wichtige Folgerungen für die Theorie der Eulerschen Integrale ziehen, namentlich in bezug auf die Fälle, in denen sie sich ohne Hilfe neuer Funktionen darstellen lassen. Da die der ersten Art auf die der zweiten zurückgeführt werden können, so beginnen wir mit der Untersuchung der letzteren. Nun ist bekannt, daß sich bestimmte Integrale jedesmal ermitteln lassen, wenn man die unbestimmten Integrale allgemein darstellen kann (vgl. Art. 6); die Integralrechnung lehrt aber, daß dies bei dem Integral

$$\int x^{\mu-1} e^{-x} \mathrm{d}x$$

nur dann möglich ist, wenn μ eine positive ganze Zahl n ist; wir können also im voraus schließen, daß dann auch $\Gamma(n)$ sich wird angeben lassen. Nun haben wir aber in der Gleichung (4) eine Reduktionsformel gewonnen, welche uns lehrt, wie eine Gammafunktion durch eine andere dargestellt werden kann, wenn ihre Argumente um eine ganze Zahl differieren; nehmen wir also am einfachsten $\mu = 1$, so erhalten wir aus der unbestimmten Integration

$$(5) \quad \Gamma(1) = \int_0^\infty e^{-x} \mathrm{d}x = 1 \text{ und folglich } \Gamma(n) = (n-1)(n-2)\ldots 2.1.$$

Dies ist aber auch der einzige Fall, in welchem a priori einleuchtet, daß $\Gamma(\mu)$ sich darstellen läßt.

Einen ähnlichen Weg können wir auch bei den Eulerschen Integralen der ersten Art einschlagen, indem wir zunächst die Darstellbarkeit des unbestimmten Integrals

$$\int x^{a-1}(1-x)^{b-1}\,\mathrm{d}\,x$$

untersuchen; dieses gehört bekanntlich zu der Klasse der Integrale von sogenannten binomischen Differentialen, welche unter der allgemeinen Form

$$\int x^m(a+b\,x^n)^p\,\mathrm{d}\,x$$

stehen; es ist aber bekannt, daß das binomische Differential jedesmal rational und folglich auch integrabel gemacht werden kann, wenn entweder $\frac{m+1}{n}$ oder $\frac{m+1}{n}+p$ eine ganze Zahl ist, und m, n und p rational sind. Damit also das obige unbestimmte Integral darstellbar sei, muß entweder a [oder auch b, da ja $B(a,b)=B(b,a)$ ist] oder $a+b$ eine ganze Zahl sein. Der erste Fall folgt aber auch unmittelbar aus den Formeln (2) und (4); denn wenn a eine ganze Zahl m ist, so geben diese Formeln

$$B(m,b)=\frac{\Gamma(m)\Gamma(b)}{\Gamma(m+b)}=\frac{\Gamma(m)}{(m-1+b)(m-2+b)\ldots(1+b)b}$$

und folglich mit Hilfe von der Formel (5)

$$(6)\qquad B(m,b)=\frac{(m-1)(m-2)\ldots 2.1}{(m-1+b)(m-2+b)\ldots(1+b)b}.$$

Ebenso erhält man, wenn n eine positive ganze Zahl bedeutet:

$$B(a,n)=\frac{(n-1)(n-2)\ldots 2.1}{(n-1+a)(n-2+a)\ldots(1+a)a};$$

$$B(m,n)=\frac{(m-1)\ldots 2.1.(n-1)\ldots 2.1}{(m+n-1)(m+n-2)\ldots 2.1}.$$

Dagegen liefert der zweite Fall, in welchem $a+b$ eine ganze Zahl, ohne daß a und b gleichzeitig ganze Zahlen sind, unabhängig von den Eulerschen Integralen der zweiten Art, eine neue Klasse von Integralen, von denen man a priori behaupten kann, daß sie sich darstellen lassen; doch können sie alle folgendermaßen auf ein einziges zurückgeführt werden. Ist nämlich $a+b$ eine ganze positive Zahl (positive, weil als bekannt vorauszusetzen ist, daß die Eulerschen Integrale für negative Argumente stets unendlich groß aus-

fallen), so kann man immer $a = m + r$, $b = n - r$ setzen, worin m und n positive ganze Zahlen, und r ein positiver echter Bruch ist. Mit Benutzung der Reduktionsformel (4) findet man dann leicht

$$B(m+r, n-r) = \frac{\Gamma(m+r)\,\Gamma(n-r)}{\Gamma(m+n)}$$

$$= \frac{(m-1+r)(m-2+r)\ldots r\Gamma(r).(n-1-r)(n-2-r)\ldots(1-r)\Gamma(1-r)}{(m+n-1)(m+n-2)\ldots 3.2.1}$$

oder, da aus den Gleichungen (2) und (5) $\Gamma(r)\,\Gamma(1-r) = B(r, 1-r)$ folgt,

$$(7) \quad B(m+r, n-r) = \frac{(m-1+r)\ldots r.(n-1-r)\ldots(1-r)}{(m+n-1)(m+n-2)\ldots 2.1}\,B(r, 1-r).$$

Das Integral $B(r, 1-r)$, auf welches hierdurch die Integrale

$$B(m+r,\ n-r)$$

zurückgeführt werden, ist eines der interessantesten der Integralrechnung und namentlich von der größten Wichtigkeit für die Theorie der Eulerschen Integrale beider Arten, wie schon aus der letzten Gleichung hervorgeht. So einfach aber die Form ist, in welcher der Wert desselben dargestellt werden kann, so verschiedenartig untereinander und kompliziert sind die Methoden, welche diesen Wert kennen lehren. Mit diesem Integral sollen sich daher die folgenden Artikel beschäftigen.

3.

Der Gleichmäßigkeit in der Bezeichnung wegen will ich b statt r schreiben, und $B(b, 1-b) = \Gamma(b)\,\Gamma(1-b)$ kurz mit B bezeichnen, so daß B als Funktion der einen Veränderlichen b aufgefaßt wird; zwischen b und B besteht also folgende Gleichung:

$$(8) \quad \left\{ \begin{array}{l} B = \displaystyle\int_0^1 \left(\frac{x}{1-x}\right)^b \frac{\mathrm{d}x}{x} = \int_0^1 \left(\frac{x}{1-x}\right)^{1-b} \frac{\mathrm{d}x}{x} \\ \quad = \displaystyle\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{x+1} = \int_0^\infty \frac{x^{-b}\,\mathrm{d}x}{x+1} \end{array} \right.$$

Die beiden letzten Formen erhält man, wenn man in den beiden ersten x für $\frac{x}{1-x}$ schreibt. Wenn nun schon im vorigen Artikel b auf das Intervall zwischen 0 und 1 beschränkt ist, weil sonst das Integral B als Eulersches Integral ein negatives Argument und da-

mit einen unendlich großen Wert erhielte, so soll in diesem Artikel die Notwendigkeit dieser Beschränkung unabhängig von der Theorie der Eulerschen Integrale in aller Strenge erwiesen werden. Größerer Allgemeinheit wegen will ich diese Untersuchung nicht unmittelbar an das Integral B, sondern an das allgemeinere

$$\int_0^\infty \frac{1+x+xx+\cdots+x^{m-1}}{1+x+xx+\cdots+x^{n-1}} x^{b-1}\,dx = \int_0^\infty \frac{1-x^m}{1-x^n} x^{b-1}\,dx$$

anknüpfen, welches für $m = 1$, $n = 2$ in das Integral B übergeht. Die Form rechts erfordert auch nicht einmal, daß m und n ganze Zahlen sind; ich will daher gleich zu der Betrachtung des Integrals

$$\varphi(b) = \int_0^\infty \frac{1-x^\mu}{1-x^\nu} x^{b-1}\,dx, \tag{9}$$

worin b, μ, ν beliebige reelle Konstanten bedeuten sollen, übergehen.

Zuerst wird man leicht einsehen, daß man μ und ν stets positiv annehmen darf, ohne die Allgemeinheit des Integrals zu beeinträchtigen, indem man statt $1-x^\mu$ und $1-x^\nu$ auch $x^\mu(x^{-\mu}-1)$ und $x^\nu(x^{-\nu}-1)$ schreiben kann. Zerlegt man dann $\varphi(b)$ in zwei Integrale von derselben Funktion, deren Grenzen bzw. 0, 1 und 1, ∞ sind, und setzt in dem zweiten Integral $\frac{1}{x}$ für x, so erhält auch dieses die Grenzen 0, 1, und beide lassen sich in

$$\varphi(b) = \int_0^1 \frac{1-x^\mu}{1-x^\nu}(x^b + x^{\nu-\mu-b})\frac{dx}{x} \tag{10}$$

zusammenziehen. Da nun nach der Voraussetzung μ und ν positiv sind, so ist innerhalb der Integrationsgrenzen für x, d. h. wenn x ein positiver echter Bruch ist, der Quotient $\frac{1-x^\mu}{1-x^\nu}$ fortwährend eine positive endliche Zahl; denn auch für $x = 1$ erhält dieser Quotient einen endlichen Wert, nämlich $\frac{\mu}{\nu}$. Bezeichnet man daher den größten und kleinsten Wert desselben mit M und N, so sind dies ebenfalls endliche positive Zahlen, und es ist im ganzen Integrationsintervall

$M > \frac{1-x^\mu}{1-x^\nu} > N$, und folglich auch, nach einem bekannten Satze aus der Theorie der bestimmten Integrale

$$M\int_0^1 (x^b + x^{\nu-\mu-b})\frac{\mathrm{d}x}{x} > \varphi(b) > N\int_0^1 (x^b + x^{\nu-\mu-b})\frac{\mathrm{d}x}{x}.$$

Da nun das Integral, welches zu beiden Seiten von $\varphi(b)$ mit den Faktoren M und N vorkommt, die Werte $\frac{\nu-\mu}{b(\nu-\mu-b)}$, $\pm\infty$, oder $-\infty$ erhält, je nachdem sowohl b als $\nu-\mu-b$ positiv, oder eins von beiden 0, oder negativ ist, so folgt, daß nur im ersten Falle $\varphi(b)$ einen endlichen, und zwar positiven, in jedem andern aber einen unendlich großen Wert erhält; es ist daher erforderlich, daß sowohl b als auch $\nu-\mu-b$ eine positive Zahl sei, was man durch die Bedingung $\nu-\mu > b > 0$ ausdrücken kann; hieraus geht zugleich hervor, daß $\nu > \mu$ sein muß. Wird $b = 0$ oder $b = \nu-\mu$, so wird $\varphi(b)$ nicht nur unendlich groß, sondern auch unstetig, indem $\varphi(b)$ von $+\infty$ in $-\infty$ überspringt.

Aus der Gleichung (10) läßt sich noch eine interessante Folgerung ziehen; setzt man nämlich $\nu-\mu-b$ statt b, so erhält man unmittelbar

$$\varphi(\nu-\mu-b) = \varphi(b), \tag{11}$$

und wenn man hierin $b = \frac{\nu-\mu}{2} + b'$ setzt, in bezug auf b' differentiiert und dann $b' = 0$ setzt, so folgt $\varphi'\left(\frac{\nu-\mu}{2}\right) = 0$, worin $\varphi'(b) = \frac{\mathrm{d}\varphi(b)}{\mathrm{d}b}$ ist; um zu entscheiden, ob der Wert $b = \frac{\nu-\mu}{2}$ einem Maximum oder Minimum von $\varphi(b)$ entspricht, muß man das zweite Differentialverhältnis $\varphi''(b)$ bilden; da dieses durch das Integral

$$\int_0^\infty \frac{1-x^\mu}{1-x^\nu}\, x^{b-1}\,\mathrm{d}x\,(lx)^2$$

dargestellt wird, worin lx den natürlichen Logarithmen von x bezeichnet, und folglich in dem ganzen Intervall von b positiv ist, so

wird $\varphi\left(\frac{\nu-\mu}{2}\right)$ ein Minimum von $\varphi(b)$ sein, und zwar das einzige. Dieses Minimum wird demnach

$$(12) \qquad \varphi\left(\frac{\nu}{2}-\frac{\mu}{2}\right)=\int_0^\infty \frac{x^{\frac{\mu}{2}}-x^{-\frac{\mu}{2}}}{x^{\frac{\nu}{2}}-x^{-\frac{\nu}{2}}}\,\frac{\mathrm{d}x}{x}=2\int_0^\infty \frac{x^{\mu}-x^{-\mu}}{x^{\nu}-x^{-\nu}}\,\frac{\mathrm{d}x}{x}.$$

Wenden wir das Bisherige auf unseren Fall an, in welchem $\mu=1$, $\nu=2$ zu setzen ist, so ergibt sich, daß das Integral B nur dann einen endlichen, und zwar positiven Wert besitzt, wenn b ein positiver echter Bruch ist; ferner das $B=\varphi(b)=\varphi(1-b)$ ist und für $b=\frac{1}{2}$ ein Minimum

$$(13) \qquad \varphi\left(\tfrac{1}{2}\right)=2\int_0^\infty \frac{x-\frac{1}{x}}{xx-\frac{1}{xx}}\,\frac{\mathrm{d}x}{x}=2\int_0^\infty \frac{\mathrm{d}x}{xx+1}=\pi$$

erreicht.

4.

Es sollen jetzt die hauptsächlichsten Beweise angegeben werden, welche bisher für den Wert des Integrals B aufgestellt sind; indessen wird es genügen, kurz den Gang derselben anzudeuten, und nur da, wo eine strengere Begründung nötig scheint, näher ins Detail zu gehen.

Da schon in Art. 2 gezeigt ist, daß sich der Wert des Integrals $B(m+r, n-r)$, von welchem B nur ein spezieller Fall ist, aus der unbestimmten Integration ergeben muß, wenn r ein echter rationaler Bruch ist, so ist es am natürlichsten, mit dieser Methode den Anfang zu machen. Nimmt man daher $b=\frac{m}{n}$ an, worin m und n positive ganze Zahlen sind, und $m<n$, so kommt es zunächst darauf an, in dem Integral

$$(14) \qquad B=\int_0^\infty \frac{x^{b-1}\mathrm{d}x}{x+1}=\int_0^\infty \frac{x^{\frac{m}{n}-1}\mathrm{d}x}{x+1}=n\int_0^\infty \frac{x^{m-1}\mathrm{d}x}{x^n+1}$$

die unbestimmte Integration auszuführen, welche bekanntlich die Zerlegung der unter dem Integralzeichen stehenden Funktion in Partialbrüche erfordert. Setzt man zur Abkürzung $\vartheta = e^{\frac{\pi}{n} i}$, worin $i = \sqrt{-1}$ ist, so ist

$$x^n + 1 = (x - \vartheta)(x - \vartheta^3) \ldots (x - \vartheta^{2k-1}) \ldots (x - \vartheta^{2n-1});$$

führt man danach die Zerlegung in Partialbrüche mit linearen Nennern und die Integration jedes einzelnen Gliedes aus, so findet man

$$(15) \qquad n \int \frac{x^{m-1}\,dx}{x^n + 1} = -\sum_{k=1}^{k=n} \vartheta^{m(2k-1)}\, l(\vartheta^{2k-1} - x).$$

Die Summe rechts kann man auch so schreiben:

$$-\sum_{k=1}^{k=n} \vartheta^{m(2k-1)}\; l\left(\frac{\vartheta^{2k-1}}{x} - 1\right) - lx \cdot \sum_{k=1}^{k=n} \vartheta^{m(2k-1)},$$

worin $\Sigma \vartheta^{m(2k-1)} = \vartheta^m \Sigma (\vartheta^{2m})^{k-1} = \vartheta^m \dfrac{\vartheta^{2mn} - 1}{\vartheta^{2m} - 1} = 0$ ist, so daß auch

$$(16) \qquad n \int \frac{x^{m-1}\,dx}{x^n + 1} = -\sum_{k=1}^{k=n} \vartheta^{m(2k-1)}\; l\left(\frac{\vartheta^{2k-1}}{x} - 1\right)$$

ist; hierbei ist wohl zu bemerken, daß die Summen in (15) und (16) vollkommen gleich, nicht etwa um eine Konstante verschieden sind. Setzt man daher in (16) $x = \infty$ und in (15) $x = 0$, so gibt die Differenz das bestimmte Integral B, nämlich

$$(17) \qquad \begin{cases} B = \sum_{k=1}^{k=n} \vartheta^{m(2k-1)}\; l(\vartheta^{2k-1}) \\ = \frac{\pi i}{n} \sum_{k=1}^{k=n} (2k-1)\, \vartheta^{m(2k-1)} = \frac{\pi}{\sin b\pi}, \end{cases}$$

womit also der Wert von B für rationale b gefunden ist. Durch die Umformung von (15) in (16) glaube ich am kürzesten gezeigt zu haben, daß die Summe in (15) für $x = \infty$ verschwindet, und hinsichtlich seiner Strenge scheint dieser Weg denen wenigstens nicht nachzustehen, welche in den meisten Lehrbüchern der Integralrechnung befolgt sind.

5.

Ein zweiter Beweis ist der folgende, welcher, so viel mir bekannt ist, von Schlömilch gegeben ist. Aus der Gleichung

$$B = \int_0^1 \frac{x^{b-1} + x^{-b}}{x+1}\,\mathrm{d}x,$$

welche sich aus der Formel (10) in Art. 3 ergibt, wenn man $\mu = 1$, $\nu = 2$ setzt, erhält man durch Entwicklung von $\frac{1}{x+1}$ nach Potenzen von x mit Berücksichtigung des Restes und durch Ausführung der Integrationen für B die $n$gliedrige Reihe

$$(18)\quad \frac{1}{b} + \frac{2b}{1-bb} - \frac{2b}{4-bb} + \frac{2b}{9-bb} - \cdots + (-1)^n \frac{2b}{(n-1)^2 - bb}$$

nebst dem Reste

$$\frac{(-1)^{n-1}}{n-b} + (-1)^n \int_0^1 \frac{(x^{b-1} + x^{-b})\,x^n}{x+1}\,\mathrm{d}x.$$

Durch ähnliche Betrachtungen, wie die in Art. 3 über die Endlichkeit von $\varphi(b)$ angestellten, läßt sich zeigen, daß dieser Rest für unendlich wachsende n gleich Null wird, so daß B der unendlich fortgesetzten Reihe (18) gleich zu setzen ist. Nimmt man aber in der als bekannt vorausgesetzten Formel

$$\mathrm{cosec}\, u = \frac{1}{u} + \frac{2u}{\pi\pi - uu} - \frac{2u}{4\pi\pi - uu} + \text{usw.}$$

$u = bx$, so findet man unmittelbar für B denselben Wert, wie im vorigen Artikel.

6.

Ein dritter Beweis (von Cauchy) stützt sich auf einen Satz über die sogenannte Umkehrung der Integrationsordnung bei Doppelintegralen. Da die hierhergehörigen Betrachtungen sehr feiner Natur sind, und sich öfters noch Unklarheiten darüber finden, so möge es mir vergönnt sein, hier etwas weiter auszuholen, um ein sicheres Fundament für diese Untersuchung zu gewinnen. Dazu ist aber erforderlich, auf die Grundlagen der Theorie der bestimmten Integrale zurückzugehen.

Das bestimmte Integral wird meistens definiert als Differenz zweier Werte des unbestimmten Integrals, welche zwei speziellen

Werten der Integrationsvariabelen entsprechen; die letztern heißen die Grenzen des Integrals. So einfach aber diese Definition scheint, so wenig kann sie strengeren Anforderungen Genüge leisten, die immer gemacht werden müssen, wenn es sich um die Festlegung einer Basis für eine ganze Theorie handelt. Der Hauptgrund für die Verwerfung dieser Definition liegt vorzüglich in dem Umstande, daß sie nicht unmittelbar auf der eigentlich gegebenen Funktion fußt, sondern als Mittelglied noch eine andere Funktion, nämlich das unbestimmte Integral voraussetzt; und dies ist ein Übelstand in mehrfacher Hinsicht. Einmal ist die Existenz des bestimmten Integrals nicht eher evident, als bis die des unbestimmten nachgewiesen ist; gesetzt aber auch, daß dies allgemein möglich wäre, so fragt sich andererseits, ob nach dieser Definition das bestimmte Integral wirklich ein bestimmtes zu nennen ist, d. h. ob es nur von der gegebenen Funktion und den Grenzen abhängt. Es ist schon mehrfach gezeigt, daß dies keineswegs der Fall ist, und es sind Fälle bekannt, in welchen diese Definition zu Zweideutigkeiten führt, welche auf diesem Wege allein gar nicht zu heben sind. Ich hoffe nun zeigen zu können, daß das nach dieser Definition aufgefaßte bestimmte Integral in jedem Falle vollkommen so unbestimmt ist wie das sogenannte unbestimmte Integral.

Während nämlich die obige Definition schon zu Zweifeln Anlaß gibt, wenn es nicht möglich ist, mit Hilfe der bekannten Methoden das unbestimmte Integral darzustellen, so geschieht dies noch in viel höherem Maße, wenn es mehrere, ja unendlich viele Funktionen gibt, deren Differential die gegebene Funktion ist. Es läßt sich zwar strenge beweisen, daß diese Funktionen nur um sogenannte Konstanten voneinander verschieden sein können, und darauf fußt gerade die obige Definition, indem sie stillschweigend voraussetzt, daß der konstante Unterschied solcher Funktionen wirklich für alle Werte der Veränderlichen derselbe bleibt. Aber gerade dies ist durchaus nicht notwendig; man kann sich hingegen denken, daß diese Konstante in verschiedenen endlichen Intervallen der Veränderlichen x verschiedene Werte besitzt, und doch wird in jedem das Differentialverhältnis von $f(x) + C$ dieselbe Funktion $f'(x)$ sein, vorausgesetzt daß C seinen Wert nicht stetig mit x verändert, weil dann C nicht mehr eine Konstante wäre. Dies leuchtet namentlich geometrisch ein, wenn man $f(x)$ als Ordinate einer krummen Linie betrachtet; man kann beliebige Stücke dieser Linie parallel der Ordinatenachse

verschieben, ohne daß dadurch $f'(x)$ geändert würde. Mit andern Worten, das erste Differentialverhältnis einer Funktion gibt nicht den geringsten Aufschluß über die Stetigkeit derselben. Solche Unstetigkeiten lassen sich auch analytisch darstellen, namentlich mit Hilfe der Fourierschen Integrale, noch einfacher aber mit ganz elementaren Hilfsmitteln.

Bei der Zweideutigkeit, welche jeder Quadratwurzel hinsichtlich ihres Zeichens anhaftet, ist es durchaus erforderlich, durch ein bestimmtes Zeichen immer nur die eine Wurzel zu bezeichnen. So ist man auch darin übereingekommen, unter $\sqrt{x}$ stets die positive Quadratwurzel aus x zu verstehen. Die Notwendigkeit hiervon leuchtet namentlich ein, wenn statt einer Wurzelgröße ein anderer Ausdruck, z. B. die binomische Reihe gesetzt wird, welche jedenfalls immer nur eine Wurzel ausdrückt. Dies vorausgesetzt, läßt sich leicht ein Ausdruck bilden, welcher zwar mit x sich nicht stetig ändert, also eine Konstante ist, aber doch in verschiedenen Intervallen verschiedene Werte erhält. Ein solcher Ausdruck ist z. B. $C\frac{x-c}{\sqrt{(x-c)^2}}$, welcher gleich $+C$ oder $-C$ ist, je nachdem x größer oder kleiner als c genommen wird. Durch Differentiation findet man natürlich

$$\frac{\mathrm{d}\left(C\frac{x-c}{\sqrt{(x-c)^2}}\right)}{\mathrm{d}x} = C\frac{\sqrt{(x-c)^2}-(x-c)\frac{x-c}{\sqrt{(x-c)^2}}}{(x-c)^2} = 0$$

und folglich ist auch

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(f(x)+C\frac{x-c}{\sqrt{(x-c)^2}}\right) = \frac{\mathrm{d}f(x)}{\mathrm{d}x} = f'(x).$$

Wollte man daher die obige Definition des bestimmten Integrals zur Anwendung bringen, so müßte man aus dem unbestimmten Integral

$$\int f'(x)\mathrm{d}x = f(x)+C\frac{x-c}{\sqrt{(x-c)^2}}$$

das bestimmte Integral

$$\int_a^b f(x)\mathrm{d}x = f(b)-f(a)+C\frac{b-c}{\sqrt{(b-c)^2}}-C\frac{a-c}{\sqrt{(a-c)^2}}$$

erhalten; nimmt man hierin $a<c<b$, so ist die Summe der beiden letzten Glieder gleich $2C$, so daß das bestimmte Integral noch eine völlig willkürliche Konstante enthält.

Hiermit ist wohl das Ungenügende dieser Definition des unbestimmten Integrals dargetan, und wir wenden uns nun zu einer anderen, welche direkt von den gegebenen Größen ausgeht; nach ihr ist nämlich das bestimmte Integral als die Summe aller der unendlich kleinen Werte des gegebenen Differentials aufzufassen, wenn man der Veränderlichen x stetig alle Werte beilegt, welche zwischen den gegebenen Grenzen des Integrals liegen. Diese Definition läßt wenigstens keine anderen Zweideutigkeiten zu, als solche, welche schon in der Natur der gegebenen Funktion liegen. Es läßt sich ferner zeigen, daß sie mit der ersteren stets identisch ist, sobald nur das unbestimmte Integral so gewählt ist, daß es innerhalb des Integrationsintervalls keine Unstetigkeit enthält; denn dann ist die Summe, welche nach der zweiten Definition das Integral bildet, gerade die Summe aller der unendlich kleinen Inkremente, welche das unbestimmte Integral $f(x)$ erhält, wenn x das Intervall von a bis b stetig durchläuft. Ist aber $f(x)$ an irgend einer Stelle c zwischen a und b unstetig, so kann man sich eine stetige Funktion $f_1(x)$ substituiert denken, deren Differential ebenfalls $f'(x)\,\mathrm{d}x$ ist. Dann ist das bestimmte Integral $= f_1(b) - f_1(a)$, und diese Differenz unterscheidet sich von $f(b) - f(a)$ nur um den Betrag des Sprunges, welchen $f(x)$ an der Stelle $x = c$ macht, und es wird daher

$$\int_a^b f'(x)\,\mathrm{d}x = f(b) - f(a) + \lim\left(f(c-\delta) - f(c+\varepsilon)\right)$$

werden, worin δ und ε unendlich kleine, mit $(b-a)$ gleichstimmige Größen bedeuten; und statt dieser Gleichung kann man auch die folgende schreiben:

$$\int_a^b f'(x)\,\mathrm{d}x = \lim\left(\int_a^{c-\delta} f'(x)\,\mathrm{d}x + \int_{c+\varepsilon}^b f'(x)\,\mathrm{d}x\right).$$

7.

Die eben angestellten Betrachtungen sind vorzüglich wichtig bei solchen bestimmten Integralen, die noch eine andere Veränderliche enthalten, also bei Integralen von der Form

$$\int_a^b f(x,\xi)\,\mathrm{d}x,$$

worin ξ eine von x unabhängige Veränderliche bedeutet. Es kann nämlich der Fall eintreten, daß das unbestimmte Integral, wenn es im allgemeinen auch für alle Werte von x stetig ist, doch diese Eigenschaft verliert, wenn man der Veränderlichen ξ einen bestimmten Wert beilegt. Dies ist namentlich dann zu berücksichtigen, wenn das bestimmte Integral, als Funktion von ξ angesehen, einer zweiten Integration in bezug auf ξ unterworfen wird, und zwar zwischen Grenzen, innerhalb deren auch der spezielle Wert von ξ liegt, welcher das in bezug auf x genommene unbestimmte Integral unstetig macht. Sind α, β diese Grenzen, c und γ die Werte von x und ξ, für welche das Integral in bezug auf x unstetig wird, so muß man zufolge des vorigen Artikels

$$(19) \qquad \int_\alpha^\beta \mathrm{d}\xi \int_a^b f(x,\xi)\,\mathrm{d}x = \lim \int_\alpha^\beta \mathrm{d}\xi \int_a^{c-\varepsilon} f(x,\xi)\,\mathrm{d}x + \int_\alpha^\beta \mathrm{d}\xi \int_{c+\varepsilon}^b f(x,\xi)\,\mathrm{d}x$$

setzen; denn man muß erst die Integration in bezug auf x so ausführen, daß sie für alle Werte von ξ, welche bei der zweiten Integration in Betracht kommen, gültig bleibt. Ich habe diese Formel angeführt, um dadurch der unrichtigen Auffassung eines Satzes zu begegnen, der sich auf die Umkehrung der Integrationsordnung bei Doppelintegralen bezieht. In einem solchen Doppelintegral kann man nämlich die Ordnung vertauschen, also

$$(20) \qquad \int_\alpha^\beta \mathrm{d}\xi \int_a^b f(x,\xi)\,\mathrm{d}x = \int_a^b \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}x$$

setzen, wenn $f(x,\xi)$ für alle Werte von x und ξ innerhalb der Integration endlich und stetig bleibt; wird aber $f(x,\xi)$ für $x = c$, $\xi = \gamma$ unstetig, so kann man noch immer

$$\int_\alpha^\beta \mathrm{d}\xi \int_a^{c-\varepsilon} f(x,\xi)\,\mathrm{d}x + \int_\alpha^\beta \mathrm{d}\xi \int_{c+\varepsilon}^b f(x,\xi)\,\mathrm{d}x = \int_a^{c-\varepsilon} \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}\xi + \int_{c+\varepsilon}^b \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}\xi$$

setzen; bezeichnet man die unbestimmten Integrale in bezug auf x und ξ bzw. mit $F(x,\xi)$ und $\varphi(x,\xi)$ und setzt diese als stetig zwischen den Grenzen der einzelnen Integrale voraus, so geht die letzte Gleichung in

$$\int_\alpha^\beta [F(b,\xi) - F(a,\xi)]\,\mathrm{d}\xi - \int_\alpha^\beta [F(c+\varepsilon,\xi) - F(c-\varepsilon,\xi)]\,\mathrm{d}\xi$$
$$= \int_a^{c-\varepsilon} [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x + \int_{c+\varepsilon}^b [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x$$

über; und wenn man hierin ε Null werden läßt, so erhält man

$$(21)\quad \begin{cases} \int_\alpha^\beta [F(b,\xi) - F(a,\xi)]\,\mathrm{d}\xi - \lim \int_\alpha^\beta [F(c+\varepsilon,\xi) - F(c-\varepsilon,\xi)]\,\mathrm{d}\xi \\ \qquad = \int_a^b [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x \end{cases}$$

Diese Formel wird meistens so aufgefaßt, als gäbe das zweite Glied auf der linken Seite den Unterschied zwischen den beiden Doppelintegralen in (20) an; aus dem im Anfang dieses Artikels Gesagten erhellt aber, daß dies nicht richtig ist, indem erst beide Glieder der linken zusammengenommen das auf der linken Seite in (20) stehende Doppelintegral darstellen. Doch wird hierdurch die Richtigkeit der Gleichung (21) nicht beeinträchtigt, und diese ist es gerade, auf welche sich der von Cauchy gegebene Beweis stützt. Nimmt man nämlich

$$f(x,\xi) = if'(x+\xi i)$$

an, worin $i = \sqrt{-1}$ und $f'(z) = \dfrac{\mathrm{d}f(z)}{\mathrm{d}z}$ ist, so wird

$$F(x,\xi) = if(x+\xi i) \quad \text{und} \quad \varphi(x,\xi) = f(x+\xi i)$$

und die Gleichung (21) geht in die folgende über:

$$(22)\quad \begin{cases} i\int_\alpha^\beta [f(b+\xi i) - f(a+\xi i)]\,\mathrm{d}\xi \\ -i\lim \int_\alpha^\beta [f(c+\varepsilon+\xi i) - f(c-\varepsilon+\xi i)]\,\mathrm{d}\xi \\ \qquad = \int_a^b [f(x+\beta i) - f(x+\alpha i)]\,\mathrm{d}x. \end{cases}$$

Führt man in dem zweiten Gliede links eine neue Variabele η durch die Gleichung $\xi = \gamma + \varepsilon\eta$ ein, worin der Annahme nach $\alpha < \gamma < \beta$ ist, und setzt

$$(23)\qquad f(z) = \frac{F(z)}{z - c - \gamma i},$$

so findet man leicht

$$(24)\qquad i \lim \int_\alpha^\beta [f(c+\varepsilon+\xi i) - f(c-\varepsilon+\xi i)]\,\mathrm{d}\xi = 2\pi i F(c+\gamma i).$$

8.

Aus den eben entwickelten Formeln hat nun Cauchy den Wert des Integrals B abgeleitet, aber auf eine Weise, welche in einzelnen Punkten einer strengeren Begründung sehr bedürftig erscheint. Sie besteht in folgendem: Wenn die Funktion $f(z)$ so beschaffen ist, daß für jeden Wert von ξ $f(\pm\infty + \xi i) = 0$ und für jeden Wert von x $f(x + \infty i) = 0$ ist, so folgt aus den Gleichungen (22), (23) und (24), wenn man $\alpha = 0$, $\beta = \infty$, $a = -\infty$, $b = \infty$ setzt,

$$\int_{-\infty}^{+\infty} f(x)\,dx = 2\pi i F(c + \gamma i), \tag{25}$$

worin nun γ zufolge der Bedingung $\alpha < \gamma < \beta$ notwendig positiv sein muß. Setzt man jetzt $f(z) = \frac{(-zi)^{\mu-1}}{zz+1}$, worin μ eine zwischen 0 und 2 liegende Zahl ist (unmotiviert), so sind die Bedingungen $f(\pm\infty + \xi i) = 0$ und $f(x + \infty i) = 0$ erfüllt; die Werte von x und ξ, welche $f(x + \xi i)$ unendlich machen, sind $c = 0$, $\gamma = 1$; es ist daher

$$F(z) = (z - i)\frac{(-zi)^{\mu-1}}{zz+1}; \quad F(c + \gamma i) = F(i) = \frac{1}{2i}$$

und folglich

$$\int_{-\infty}^{+\infty} \frac{(-xi)^{\mu-1}}{xx+1}\,dx = \pi. \tag{26}$$

Zerlegt man dies Integral in zwei andere, deren Grenzen o, ∞ und $-\infty$, o sind, und setzt in dem zweiten $(-x)$ statt x, so findet man

$$\int_0^{\infty} \frac{x^{\mu-1}\,dx}{xx+1} = \frac{\pi}{(+i)^{\mu-1} + (-i)^{\mu-1}} = \frac{\pi}{2\cos(\mu-1)\frac{\pi}{2}} = \frac{\pi}{2\sin\mu\frac{\pi}{2}},$$

und hierin braucht man bloß x statt xx, und $\mu = 2b$ (wo b zwischen 0 und 1 liegt, wenn $0 < \mu < 2$ ist) zu setzen, um die Gleichung (17) wieder zu erhalten.

Hierin scheint mir namentlich die Ableitung der Gleichung (25) nicht ganz streng zu sein; denn wenn auch die Bedingungen $f(\pm\infty + \xi i) = 0$, $f(x + \infty i) = 0$ für jedes zwischen 0 und 2 liegende μ erfüllt sind (eigentlich ist dazu nur erforderlich, daß

$\mu < 3$ ist, so daß μ auch negativ sein kann), so ist doch bekannt, daß das Verschwinden der Funktion unter dem Integralzeichen das des Integrals nicht immer zur Folge hat, namentlich dann, wenn die eine Grenze unendlich groß ist. Ich will daher versuchen, durch die folgende Darstellung diese Zweifel zu heben und zugleich zu beweisen, daß μ zwischen den Grenzen 0 und 2 liegen muß.

Setzt man in der Gleichung (22) $\alpha = 0$, $b = \beta = -a = k$, so geht sie mit Berücksichtigung der Gleichung (24) in folgende über

$$i\int_0^k [f(k+\xi i) - f(-k+\xi i)]\,\mathrm{d}\xi - 2\pi i F(c+\gamma i)$$
$$= \int_{-k}^{+k} f(x+ki)\,\mathrm{d}x - \int_{-k}^{+k} f(x)\,\mathrm{d}x,$$

und wenn man in dem ersten Integral $\xi = k\eta$, im zweiten $x = ky$ setzt:

$$i\int_0^1 [f(k(1+\eta i)) - f(-k(1-\eta i))]k\,\mathrm{d}\eta - 2\pi i F(c+\gamma i)$$
$$= \int_{-1}^{+1} f(k(y+i))k\,\mathrm{d}y - \int_{-k}^{+k} f(x)\,\mathrm{d}x.$$

Wenn nun bei unendlichem Wachsen von k die Funktionen unter den Integralzeichen verschwinden, und zwar für jeden Wert der Variabelen, so werden die Integrale selbst gleich Null. Nun ist für unseren Fall

$$kf(k(1+\eta i)) = (-i)^{\mu-1}\frac{k^\mu(1+\eta i)^{\mu-1}}{k^k(1+\eta i)^2+1}$$

und ähnlich die anderen Funktionen; damit diese Ausdrücke bei dem unendlichen Wachsen von k verschwinden, ist erforderlich, daß $\mu < 2$ sei, wodurch aber nicht ausgeschlossen ist, daß μ auch negativ sein kann. Jedenfalls erhält man unter dieser Annahme die Gleichung (25). Aus dem Gange des Beweises im vorigen Artikel leuchtet aber ein, daß, wenn es mehrere Paare von Werten, wie c und γ gibt, für welche $f(x,\xi)$ unendlich wird, in Gleichung (25) die Summe der ihnen entsprechenden Ausdrücke zu nehmen ist (nur mit der Bemerkung, daß, wenn $\gamma = \alpha$ ist, in Gleichung (24) $\pi i F(c+\gamma i)$ statt $2\pi i F(c+\gamma i)$ gesetzt werden muß). In unserem Falle ist aber $f(x,\xi) = if(x+\xi i)$ und nach der obigen Spezialisierung von $f(z)$:

$$f'(z) = (-i)^{\mu-1}\frac{(\mu-3)z^\mu + (\mu-1)z^{\mu-2}}{(zz+1)^2},$$

und hierin sind die komplexen Werte von z aufzusuchen, welche diese Funktion unendlich machen; die ersten erhält man aus der Gleichung $zz + 1 = 0$, woraus die beiden Systeme $(c = 0, \gamma = 1)$ und $(c = 0, \gamma = -1)$ folgen, deren erstes oben schon behandelt ist; das zweite muß aber ausgeschlossen werden, weil dies γ der Bedingung $\alpha < \gamma < \beta$ nicht entspricht. Wenn aber, wie eben gezeigt ist, $\mu < 2$ sein muß, so ist auch $(c = 0, \gamma = 0)$ ein solches System, und wir hätten demnach noch die Korrektion $\pi i F(0)$ anzubringen, worin $F(z) = (z - c - \gamma i) f(z)$, also in diesem Falle

$$F(z) = (-i)^{\mu - 1} \frac{z^\mu}{zz + 1}$$

ist; für $z = 0$ wird $F(z)$ nun entweder unendlich groß oder Null, je nachdem μ negativ oder positiv ist. Soll daher der Wert des Integrals in (25) endlich sein, so müssen wir das letztere annehmen, und dann ist in (26) eine Korrektion nicht mehr hinzuzufügen, da $F(0) = 0$ wird. Durch diese Betrachtung ist daher die Gültigkeit der Gleichung (26), aus welcher unmittelbar der Wert des Integrals B folgt, auf die Bedingung $0 < \mu < 2$ oder $0 < b < 1$ beschränkt.

9.

Ein von den bisher angeführten wesentlich verschiedener Beweis ist endlich noch in der Abhandlung „Disquisitiones generales circa seriem infinitam etc. Auctore C. F. Gauss“ enthalten. Die ganze Anlage derselben macht es aber unmöglich, diesen Beweis hier darzustellen, indem die Grundlagen, auf welche er sich stützt, mit einem Schlage eine vollständige Theorie der Eulerschen Integrale ergeben, deshalb aber auch zu bedeutend sind, um hier bloß zu diesem einzigen Zwecke entwickelt zu werden.

Zu diesen will ich nun noch einen, so viel mir bekannt ist, neuen Beweis hinzufügen, der eben nicht viel Zurüstungen erfordert und sich stets in dem Gebiete der Integralrechnung hält, wenn auch die Methode nicht eben neu ist, die darauf hinaus läuft, die Aufgabe auf die Integration einer Differentialgleichung zweiter Ordnung zurückzuführen. Setzt man in der Gleichung

$$BB = \int_0^\infty \frac{x^{b-1}\,dx}{x+1} \int_0^\infty \frac{y^{b-1}\,dy}{y+1} = \int_0^\infty \frac{dx}{x+1} \int_0^\infty \frac{(xy)^{b-1}}{y+1}\,dy$$

$y = \frac{z}{x}$, $\mathrm{d}y = \frac{\mathrm{d}z}{x}$, kehrt dann die Integrationsordnung um, und führt die Integration in bezug auf x aus, so findet man leicht

$$BB = \int_0^\infty \frac{z^{b-1} lz}{z-1} \mathrm{d}z = \frac{\mathrm{d}}{\mathrm{d}b} \int_0^\infty \frac{z^{b-1} \mathrm{d}z}{z-1}. \tag{27}$$

Durch unbestimmte Integration in bezug auf b erhält man daher

$$\int BB \mathrm{d}b = \int_0^\infty \frac{z^{b-1} \mathrm{d}z}{z-1},$$

worin das Integral rechts sich bloß durch die Form des Nenners von dem Integral B unterscheidet; und es ist leicht vorauszusehen, daß man das Integral B wiedererhält, wenn man das eben gewonnene derselben Behandlung unterwirft. In der Tat findet man

$$B \int BB \mathrm{d}b = \int_0^\infty \frac{\mathrm{d}z}{z-1} \int_0^\infty \frac{(zy)^{b-1}}{y+1} \mathrm{d}y,$$

und wenn man $y = \frac{x}{z}$, $\mathrm{d}y = \frac{\mathrm{d}x}{z}$ setzt, dann zufolge Art. 6 und 7 das in bezug auf z genommene Integral in zwei Integrale zerlegt, deren Grenzen 0, $1-\delta$ und $1+\varepsilon$, ∞ sind, die Integrationsordnung umkehrt, und die Integration in bezug auf z ausführt, so erhält man

$$B \int BB \mathrm{d}b = \int_0^\infty \frac{x^{b-1} lx}{x+1} \mathrm{d}x + \lim \int_0^\infty \frac{x^{b-1} \mathrm{d}x}{x+1} l\left(\frac{\delta}{\varepsilon}\right).$$

Hierin ist nun zwar $\lim l\left(\frac{\delta}{\varepsilon}\right)$ unbestimmt, jedenfalls aber unabhängig von x und b, und mag mit k bezeichnet werden. Dann gibt die letzte Gleichung

$$B \int BB \mathrm{d}b = \frac{\mathrm{d}B}{\mathrm{d}b} + kB$$

oder, wenn man bedenkt, daß in dem Integral links doch schon eine willkürliche Konstante enthalten ist,

$$B \int BB \mathrm{d}b = \frac{\mathrm{d}B}{\mathrm{d}b}, \tag{28}$$

woraus man durch Division mit B und Differentiation in bezug auf b die Differentialgleichung zweiter Ordnung

$$BB = \frac{1}{B}\frac{\mathrm{d}\,\mathrm{d}B}{\mathrm{d}b^2} - \frac{1}{BB}\left(\frac{\mathrm{d}B}{\mathrm{d}b}\right)^2$$

erhält, welche die Eigentümlichkeit besitzt, daß die unabhängige Variabele b nicht vorkommt, und sich deshalb bekanntlich auf eine Differentialgleichung erster Ordnung zurückführen läßt, wenn man das erste Differentialverhältnis als neue Variabele einführt. Bezeichnen wir dieses mit B', so ist

$$\frac{\mathrm{d}B}{\mathrm{d}b} = B', \quad \frac{\mathrm{d}\,\mathrm{d}B}{\mathrm{d}b^2} = \frac{\mathrm{d}B'}{\mathrm{d}b} = \frac{B'\,\mathrm{d}B'}{\mathrm{d}B},$$

und führen wir diese Transformationen in die obige Differentialgleichung ein, so geht diese in

$$BB = \frac{B'\,\mathrm{d}B'}{B\,\mathrm{d}B} - \frac{B'B'}{BB}$$

oder in

$$\mathrm{d}(BB) = \frac{BB\,\mathrm{d}(B'B') - B'B'\,\mathrm{d}(BB)}{(BB)^2} = \mathrm{d}\,\frac{B'B'}{BB}$$

über, deren Integral

$$BB = cc + \frac{B'B'}{BB} = cc + \frac{1}{BB}\left(\frac{\mathrm{d}B}{\mathrm{d}b}\right)^2$$

ist. Zu der Bestimmung der Konstanten ist nun die Kenntnis zweier Eigenschaften des Integrals erforderlich; diese nehmen wir aus Art. 3, wo gezeigt ist, das B für $b = \frac{1}{2}$ ein Minimum $= \pi$ erreicht; da gleichzeitig $\frac{\mathrm{d}B}{\mathrm{d}b} = 0$ wird, so ergibt sich unmittelbar $cc = \pi\pi$. Man erhält dann weiter

$$\pm\,\mathrm{d}b = \frac{\mathrm{d}B}{B\sqrt{(BB - \pi\pi)}} = \frac{1}{\pi}\,\frac{-\,\mathrm{d}\,\frac{\pi}{B}}{\sqrt{\left(1 - \frac{\pi\pi}{BB}\right)}},$$

folglich durch Integration

$$\pm\,(b + c) = \frac{1}{\pi}\,arc\,cos\,\frac{\pi}{B}, \quad B = \frac{\pi}{cos\,(b + c)\pi}.$$

Da B für $b = \frac{1}{2}$ den Wert π erhält, so muß

$$cos\,(\tfrac{1}{2} + c)\pi = -\,sin\,c\pi = 1, \quad cos\,c\pi = 0$$

sein; folglich ist

$$\cos(b+c)\pi = \cos b\pi \cos c\pi - \sin b\pi \sin c\pi = \sin b\pi,$$

wodurch man wieder $B = \frac{\pi}{\sin b\pi}$ findet.

10.

Weil der im vorigen Artikel gegebene Beweis den Anforderungen der größten Strenge doch noch nicht Genüge leistet, namentlich insofern das Integral $\int_0^\infty \frac{x^{b-1}\,dx}{x-1}$ darin eine Rolle spielt, so ist es wohl nicht unangemessen, hier eine solche Modifikation noch folgen zu lassen, in welcher die unbestimmte Integration in bezug auf b ganz vermieden wird. Da die Gleichung (28) sich auch so schreiben läßt

$$\int BB\,db = \frac{dlB}{db},$$

so läßt sich vermuten, daß eine Entwicklung des rechts stehenden Ausdrucks ebenfalls zum Ziele führt. Da $B = \Gamma(b)\Gamma(1-b)$ ist, so reicht es hin, ein Integral für $\frac{dl\Gamma(\mu)}{d\mu}$ zu finden, was sich bekanntlich auf folgendem Wege erreichen läßt. Aus der Definition von $\Gamma(\mu)$ folgt

$$\frac{d\Gamma(\mu)}{d\mu} = \int_0^\infty x^{\mu-1}e^{-x}\,dx\,lx.$$

Setzt man hierin für lx das Integral

$$lx = \int_0^\infty \frac{e^{-z}-e^{-zx}}{z}\,dx,$$

welches sich aus dem Integral $\int_0^1 y^{z-1}\,dy = \frac{1}{x}$ durch Integration in bezug auf x zwischen den Grenzen 1 und x, und durch Substitution von e^{-s} für y ergibt, so findet man durch Umkehrung der Integrationsordnung und mit Hilfe von Gleichung (3) sehr leicht

$$\frac{dl\Gamma(\mu)}{d\mu} = \int_0^\infty \frac{dz}{z}\left(e^{-z} - \frac{1}{(z+1)^\mu}\right).$$

Setzt man hierin b und $(1-b)$ für μ, so ergibt sich

$$\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_0^\infty \frac{\mathrm{d}z}{z}\left(\frac{1}{(z+1)^{1-b}} - \frac{1}{(z+1)^b}\right),$$

und wenn man hierin $z = x-1$ oder $z = \frac{1}{x} - 1$ setzt:

$$\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_1^\infty \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x} = \int_0^1 \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x},$$

also auch

$$2\,\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_0^\infty \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x}.$$

Vergleicht man dies mit Gleichung (27), so ergibt sich augenblicklich

$$2\,\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_{1-b}^{b} BB\,\mathrm{d}B = 2\int_{\frac{1}{2}}^{b} BB\,\mathrm{d}b, \tag{29}$$

indem ja zufolge Art. 3 B für $b = \frac{1}{2} + b'$ und $b = \frac{1}{2} - b'$ dieselben Werte erhält; durch Differentiation dieser Gleichung in bezug auf b erhält man wieder die im vorigen Artikel behandelte Differentialgleichung.

11.

Nachdem durch die angegebenen Beweise die Richtigkeit der Gleichung

$$B(r, 1-r) = \int_0^\infty \frac{x^{r-1}\,\mathrm{d}x}{x+1} = \frac{\pi}{\sin r\pi},$$

worin r einen positiven echten Bruch bezeichnet, außer Zweifel gesetzt ist, ergibt sich unmittelbar aus Art. 2, daß die Eulerschen Integrale der ersten Art, deren beide Argumente eine ganze positive Zahl zur Summe haben, sich wirklich darstellen lassen; man findet

$$\left\{\begin{array}{l} B(m+r, n-r) \\ = \dfrac{(m+r-1)\cdots(1+r)r\cdot(n-1-r)\cdots(2-r)(1-r)}{(m+n-1)(m+n-2)\cdots 2\cdot 1}\,\dfrac{\pi}{\sin r\pi}. \end{array}\right. \tag{30}$$

Man kann hiervon auch noch einen wichtigen Rückschluß auf die Eulerschen Integrale der ersten Art machen; setzt man nämlich $m = 0$, $n = 1$, $r = \frac{1}{2}$, so findet man

$$\Gamma\left(\frac{1}{2}\right) = \int_0^\infty e^{-z} \frac{\mathrm{d}x}{\sqrt{x}} = 2\int_0^\infty e^{-xx}\,\mathrm{d}x = \sqrt{\pi} \tag{31}$$

und folglich nach Gleichung (4):

$$\Gamma\left(n + \frac{1}{2}\right) = (2n-1)(2n-3)\ldots 5.3.1\,\frac{\sqrt{\pi}}{2^n}. \tag{32}$$

12.

Nachdem in Artt. 2 und 11 die Fälle zusammengestellt sind, in welchen die Eulerschen Integrale beider Arten ohne Hilfe neuer Funktionen dargestellt werden können, will ich zum Schluß noch einmal zu dem Integral B zurückkehren, um noch einige Beziehungen desselben zu anderen Integralen zu entwickeln. Unter den verschiedenen Formen, in welchen es auftritt, sind die beiden folgenden

$$\int_{-\infty}^{+\infty} \frac{e^{(2b-1)z} + e^{-(2b-1)z}}{e^z + e^{-z}}\,\mathrm{d}z \quad \text{und} \quad 2\int_0^{\frac{\pi}{2}} (tg\,\varphi)^{2b-1}\,\mathrm{d}\varphi = 2\int_0^{\frac{\pi}{2}} (tg\,\varphi)^{1-2b}\,\mathrm{d}\varphi$$

ganz interessant; wichtiger sind aber die Verallgemeinerungen desselben durch Einführung neuer Konstanten. Dahin gehört das Integral

$$\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{x+c} = \frac{\pi c^{b-1}}{\sin b\pi}, \tag{33}$$

worin c positiv sein muß; doch läßt sich nachträglich beweisen, daß c auch imaginär sein darf; multipliziert man nämlich Zähler und Nenner der Funktion $\frac{x^{b-1}}{x+i}$ mit $(x \mp i)$, so zerfällt das entsprechende Integral in zwei andere, welche sich durch die Substitution $xx = y$ auf das Integral B reduzieren lassen, und so findet man die Gültigkeit der Gleichung (33) für imaginäre c. Durch Differentiation und Integration in bezug auf c kann man dann wieder eine Reihe von anderen Integralen ableiten.

Sind $c_1, c_2, \ldots, c_n$ voneinander verschiedene positive oder imaginäre Konstanten, ferner $0 < b < n$ und

$$f(x) = (x + c_1)(x + c_2) \ldots (x + c_n), \quad f'(x) = \frac{\mathrm{d}f(x)}{\mathrm{d}x},$$

so findet man auch

$$\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{f(x)} = \frac{\pi}{\sin b\pi} \sum_{k=1}^{k=n} \frac{c_k^{b-1}}{f'(-c_k)}, \tag{34}$$

indem man $\frac{x^\beta}{f(x)}$ in Partialbrüche zerlegt, worin β die größte in b enthaltene ganze Zahl bedeutet.

Ein Vorzug des in Art. 10 gegebenen Beweises besteht auch noch darin, daß er unmittelbar eine verwandte Klasse von Integralen bestimmen lehrt. Aus den Gleichungen (27) und (29) folgt nämlich unmittelbar

$$\int_0^\infty \frac{x^b - x^{\frac{1}{2}}}{1 - x} \frac{\mathrm{d}x}{x} = \pi \cot b\pi,$$

folglich auch

$$\int_0^\infty \frac{x^a - x^b}{1 - x} \frac{\mathrm{d}x}{x} = \pi(\cot a\pi - \cot b\pi), \tag{35}$$

und hieraus ergiebt sich auch das in Art. 3 mit $\varphi(b)$ bezeichnete Integral

$$\int_0^\infty \frac{1 - x^\mu}{1 - x^\nu} x^{b-1}\,\mathrm{d}x = \frac{1}{\nu} \int_0^\infty \frac{x^{\frac{b}{\nu}} - x^{\frac{\mu+b}{\nu}}}{1 - x} \frac{\mathrm{d}x}{x}$$

$$= \frac{\pi}{\nu} \frac{\sin\frac{\mu\pi}{\nu}}{\sin\frac{b\pi}{\nu} \sin\frac{(\mu+b)\pi}{\nu}} = \frac{2\pi}{\nu} \frac{\sin\frac{\mu\pi}{\nu}}{\cos\frac{\mu\pi}{\nu} - \cos\frac{(\mu+2b)\pi}{\nu}}$$

und das Minimum desselben

$$\int_0^\infty \frac{x^{\frac{\mu}{2}} - x^{-\frac{\mu}{2}}}{x^{\frac{\nu}{2}} - x^{-\frac{\nu}{2}}} \frac{\mathrm{d}x}{x} = \frac{2\pi}{\nu} tg\,\frac{\mu\pi}{2\nu}.$$

Die meisten der hierher gehörigen Integrale finden sich in der im Auftrage des preußischen Ministeriums von Minding herausgegebenen „Sammlung von Integraltafeln“ (Berlin 1849), im Anfang der vierten Abteilung. Vielleicht ist hier der Ort, um einige Fehler, welche sich daselbst finden, anzuzeigen und zu verbessern. Durch Zerlegung von $\frac{1}{(x-1)(x+c)}$ in Partialbrüche und Anwendung der Formeln dieses Artikels findet man leicht

$$\int_0^\infty \frac{x^a - 1}{(x-1)(x+c)}\,\mathrm{d}x = \frac{\pi}{c+1}\left(\frac{c^a - \cos a\pi}{\sin a\pi} - \frac{lc}{\pi}\right),$$

und diese Gleichung gilt für positive und negative echt gebrochene a, wovon man sich leicht überzeugt, wenn man $\frac{1}{x}$ und $\frac{1}{c}$ statt x und c schreibt. Differentiiert man in bezug auf a und setzt dann $a = 0$, so erhält man eine Reihe von Integralen, welche in jenen Tafeln unrichtig angegeben sind. Um die lästigen Differentiationen möglichst zu erleichtern, kann man folgenden Kunstgriff anwenden. Setzt man

$$\frac{lc}{\pi} + \frac{c+1}{\pi}\int_0^\infty \frac{x^a - 1}{(x-1)(x+c)}\,\mathrm{d}x = \frac{c^a - \cos a\pi}{\sin a\pi} = J, \quad \frac{\mathrm{d}^n J}{\mathrm{d}a^n} = \overset{n}{J},$$

so erhält man für $a = 0$

$$\int_0^\infty \frac{(lx)^n\,\mathrm{d}x}{(x-1)(x+c)} = \frac{\pi}{c+1}\,\overset{n}{J}_0.$$

Man findet aber leicht

$$J\pi^n \sin\left(a + \frac{n}{2}\right)\pi + n\overset{1}{J}\pi^{n-1}\sin\left(a + \frac{n-1}{2}\right)\pi + \cdots$$

$$\cdots + n\overset{n-1}{J}\pi \sin\left(a + \tfrac{1}{2}\right)\pi + \overset{n}{J}\sin a\pi$$

$$= \frac{\mathrm{d}^n(J\sin a\pi)}{\mathrm{d}\pi^n} = c^a(lc)^n - \pi^n\cos\left(a + \frac{n}{2}\right)\pi,$$

und für $a = 0$ erhält man Rekursionsformeln für die J_0 mit geraden und die mit ungeraden Indizes. So findet man

$$\int_0^\infty \frac{lx\,dx}{(x-1)(x+c)} = \frac{(lc)^2 + \pi\pi}{2(c+1)},$$

$$\int_0^\infty \frac{(lx)^2\,dx}{(x-1)(x+c)} = \frac{lc((lc)^2 + \pi\pi)}{3(c+1)},$$

$$\int_0^\infty \frac{(lx)^3\,dx}{(x-1)(x+c)} = \frac{((lc)^2 + \pi\pi)^2}{4(c+1)},$$

$$\int_0^\infty \frac{(lx)^4\,dx}{(x-1)(x+c)} = \frac{lc((lc)^2 + \pi\pi)(3(lc)^2 + 7\pi\pi)}{5(c+1)\cdot 3},$$

$$\int_0^\infty \frac{(lx)^5\,dx}{(x-1)(x+c)} = \frac{((lc)^2 + \pi\pi)^2((lc)^2 + 3\pi\pi)}{6(c+1)},$$

während in jenen Tafeln statt der Divisoren 2, 3, 4, 5, 6 die Divisoren $1\cdot 2$, $1\cdot 2\cdot 3$, $1\cdot 2\cdot 3\cdot 4$, $1\cdot 2\cdot 3\cdot 4\cdot 5$, $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6$ angegeben sind.

II.

Über ein Eulersches Integral.

[Journal für reine und angewandte Mathematik, Bd. 45, S. 370—374 (1853)].

Die von Gauß und Legendre in die Analysis eingeführten Funktionen Π und Γ stehen bekanntlich in dem Zusammenhange, daß $\Gamma(a)$ mit $\Pi(a-1)$ identisch ist, so lange a einen positiven Wert hat; für negative a ist $\Gamma(a)$ stets unendlich groß, während $\Pi(a-1)$ eine bestimmte Funktion bleibt und nur dann unendlich und unstetig wird, wenn a einen der Werte 0, -1, -2 usw. erhält. Die Funktion Π wird als unendliches Produkt, Γ als bestimmtes Integral definiert. Unstreitig ist die erstere Definition umfassender und gewährt eine tiefere Einsicht in das wahre Wesen dieser Funktionen; indessen ist es für die Integralrechnung wichtig, ohne Hilfe jener Entwicklungen in unendliche Produkte und Reihen, selbständig eine Theorie dieser Funktionen aufzustellen. Dies ist auch in der Tat nach und nach vollständig gelungen, seitdem namentlich Dirichlet (im 15. Bande dieses Journals) das berühmte Multiplikationstheorem von Gauß so elegant bewiesen hat. In dieser Abhandlung wird auch der Lehrsatz

$$\Pi(a-1)\cdot\Pi(-a)=\int_0^\infty \frac{x^{a-1}\,dx}{x+1}=\frac{\pi}{\sin a\pi}$$

angewendet, für welchen sehr verschiedene Beweise von verschiedenen Mathematikern gegeben sind, die aber fast alle ihren Weg über Entwicklungen in unendliche Reihen nehmen. In meiner, Ostern 1852 gedruckten Inaugural-Dissertation (Über die Elemente der Theorie der Eulerschen Integrale) sind die hauptsächlichsten zusammengestellt; auch habe ich schon dort einen neuen Weg hinzugefügt, welcher sich ganz im Gebiet der bestimmten Integrale hält, dem ich aber eine vollkommene Strenge nur dadurch zu verleihen vermochte, daß ich die Entstehung dieses Integrals aus der Multiplikation von $\Pi(a-1)$ und $\Pi(-a)$, und den Ausdruck für $\frac{d\log\Pi(a)}{da}$ als bekannt voraussetzte. Im folgenden soll nun ein, zwar auf ganz derselben Idee beruhender, aber von anderen Theorien ganz unabhängiger

Beweis gegeben werden, der nur die allgemeinsten Sätze über die bestimmten Integrale zu Hilfe nimmt.

Zuerst muß an einen Hilfssatz erinnert werden, der nachher einige Male gebraucht wird. Es ist bekanntlich

$$\int \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log\left(\frac{\alpha w+\beta}{\alpha' w+\beta'}\right)}{\alpha\beta'-\alpha'\beta},$$

wo die Logarithmen hyperbolische sind. Sind nun $\frac{\beta}{\alpha}$ und $\frac{\beta'}{\alpha'}$ positive Größen, so folgt hieraus

$$\int_0^\infty \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log\frac{\alpha\beta'}{\alpha'\beta}}{\alpha\beta'-\alpha'\beta}$$

oder, wenn der Logarithme immer nur von dem absoluten Werte genommen wird:

$$(1) \qquad \int_0^\infty \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log(\alpha\beta') - log(\alpha'\beta)}{\alpha\beta'-\alpha'\beta};$$

und diese Gleichung gilt selbst für den Fall, in welchem $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$ ist, wenn man den unter die Form $\frac{0}{0}$ tretenden Wert nach den Regeln der Differentialrechnung behandelt.

Gehen wir nun zu dem eigentlichen Gegenstande über, so ist erstens leicht zu sehen, daß das gegebene Integral

$$(2) \qquad \int_0^\infty \frac{x^{a-1}\,dx}{x+1} = A = \varphi(a)$$

nur dann einen endlichen, und zwar positiven Wert hat, wenn a ein positiver echter Bruch ist. Zerlegt man nämlich das Integral in zwei andere mit den Grenzen 0, 1 und 1, ∞, und schreibt im letzteren $\frac{1}{x}$ statt x, so findet man

$$(3) \qquad A = \int_0^1 \frac{x^{a-1}+x^{-a}}{x+1}\,dx.$$

Da nun im ganzen Intervall der Integration $\frac{1}{x+1}$ zwischen den Grenzen 1 und $\frac{1}{2}$ liegt, so liegt auch A zwischen den Grenzen

$$\int_0^1 (x^{a-1} + x^{-a})\,dx \quad \text{und} \quad \tfrac{1}{2}\int_0^1 (x^{a-1} + x^{-a})\,dx.$$

Dieses Integral hat aber nur dann einen endlichen und positiven Wert, $= \frac{1}{a(1-a)}$, wenn a ein positiver echter Bruch ist. Dieselbe Bedingung ist daher auch für die Endlichkeit des Integrals A nötig.

Ferner ergibt sich unmittelbar aus der Gleichung (3) der Satz

$$\varphi(a) = \varphi(1-a). \tag{4}$$

Differentiiert man diese Gleichung in bezug auf a und setzt dann $a = \frac{1}{2}$, so findet man

$$\varphi'(\tfrac{1}{2}) = 0. \tag{5}$$

Da ferner, wie leicht zu sehen, $\varphi''(\frac{1}{2})$ positiv ist, so erreicht $\varphi(a)$ für $a = \frac{1}{2}$ einen Minimumwert

$$\varphi\left(\frac{1}{2}\right) = \int_0^\infty \frac{x^{-\frac{1}{2}}\,dx}{x+1} = 2\int_0^\infty \frac{d(\sqrt{x})}{1+(\sqrt{x})^2} = \pi. \tag{6}$$

Bezeichnet w eine positive Größe, so erhält man, wenn man in der Gleichung (2) $\frac{x}{w}$ statt x schreibt:

$$\int_0^\infty \frac{x^{a-1}\,dx}{x+w} = A w^{a-1}, \tag{7}$$

und wenn man $\frac{1}{w}$ statt w setzt,

$$\int_0^\infty \frac{x^{a-1}\,dx}{xw+1} = A w^{-a}. \tag{8}$$

Multipliziert man die Gleichung (7) mit $\frac{dw}{w+1}$, integriert in bezug auf w zwischen den Grenzen 0 und ∞ und bedenkt, daß zufolge des Hilfssatzes (1)

$$\int_0^\infty \frac{dw}{(w+1)(w+x)} = \frac{\log x}{x-1}$$

ist, so erhält man

$$AA = \int_0^\infty \frac{x^{a-1}\,dx}{x-1} \log x.$$

Integriert man jetzt in bezug auf a zwischen den Grenzen $(1-a)$ und a, so erhält man

$$\int_{1-a}^{a} AA\,da = \int_0^\infty \frac{x^{a-1}-x^{-a}}{x-1}\,dx = \int_0^\infty \frac{w^{a-1}-w^{-a}}{w-1}\,dw.$$

Subtrahiert man die Gleichung (8) von (7), so findet man leicht:

$$A\frac{w^{a-1}-w^{-a}}{w-1} = \int_0^\infty \frac{x^{a-1}(x-1)}{(xw+1)(w+x)}\,dx,$$

und wenn man zwischen den Grenzen $w=0$ und $w=\infty$ integriert und erwägt, daß

$$\int_0^\infty \frac{dw}{(xw+1)(w+x)} = \frac{2\log x}{xx-1}$$

ist, so folgt unmittelbar:

$$A\int_{1-a}^{a} AA\,da = A\int_0^\infty \frac{w^{a-1}-w^{-a}}{w-1}\,dw = 2\int_0^\infty \frac{x^{a-1}\,dx}{x+1}\log x.$$

Zufolge der Eigenschaft von A, daß $A = \varphi(a) = \varphi(1-a)$ ist, ergibt sich aber

$$\int_{a-1}^{a} AA\,da = 2\int_{\frac{1}{2}}^{a} AA\,da.$$

Ferner ist

$$\int_0^\infty \frac{x^{a-1}\,dx}{x+1}\log x = \frac{dA}{da},$$

und so erhält man endlich die Gleichung

$$A\int_{\frac{1}{2}}^{a} AA\,da = \frac{dA}{da}.$$

aus welcher sich durch Division mit A und Differentiation in bezug auf a die folgende ableiten läßt:

$$AA = \frac{1}{A}\frac{dd A}{da^2} - \frac{1}{AA}\left(\frac{dA}{da}\right)^2.$$

Da in derselben die unabhängige Variable a nicht vorkommt, so führe man $\frac{dA}{da} = A'$ als neue Variable ein. Dies gibt

$$AA = \frac{A'\,dA'}{A\,dA} - \frac{A'A'}{AA}, \quad A\,dA = \frac{AA\cdot A'\,dA' - A'A'\cdot A\,dA}{A^4}$$

oder

$$d(AA) = \frac{AA\cdot d(A'A') - A'A'\cdot d(AA)}{(AA)^2},$$

und das Integral dieser Gleichung ist offenbar

$$AA = Const. + \frac{A'A'}{AA} = Const. + \frac{1}{AA}\left(\frac{dA}{da}\right)^2.$$

Um die Konstante zu bestimmen, setze man $a = \frac{1}{2}$, wofür nach Gleichung (5) und (6) $\frac{dA}{da} = 0$ und $A = \pi$ ist; daraus folgt $\pi\pi$ als Wert der Konstante und

$$da = \pm\frac{dA}{A\sqrt{(AA - \pi\pi)}} = \mp\frac{1}{\pi}\frac{d\left(\frac{\pi}{A}\right)}{\sqrt{\left(1 - \frac{\pi\pi}{AA}\right)}}.$$

Bezeichnet man mit c eine Konstante, so ergibt sich

$$a + c = \pm\frac{1}{\pi}\,arc\,cos\frac{\pi}{A}, \quad A = \frac{\pi}{cos(a+c)\pi}.$$

Um die Konstante c zu finden, setze man wieder $a = \frac{1}{2}$, woraus

$$1 = cos\left(\tfrac{1}{2}\pi + c\pi\right) = -sin\,c\pi, \quad cos\,c\pi = 0$$

und

$$cos(a+c)\pi = sin\,a\pi$$

folgt. Man erhält daher

$$A = \frac{\pi}{sin\,a\pi},$$

was zu beweisen war. Außerdem ergeben sich aus diesem Beweise sehr leicht noch mehrere verwandte Integrale, was ich hier nicht weiter ausführe.

Braunschweig, im September 1852.

III.

Ein Satz aus der Theorie der dreiachsigen Koordinatensysteme.

[Journal für reine und angewandte Mathematik, Bd. 50, S. 272—275 (1855)].

Wenn die Winkel YOZ, ZOX, XOY eines dreiachsigen Koordinatensystems durch a, b, c bezeichnet werden, so wird der konkave Winkel w zwischen zwei beliebigen Richtungen OM und OM' durch folgende Gleichung bestimmt:

$$(1)\quad \left\{\begin{array}{l} \alpha\alpha' \sin a^2 + \beta\beta' \sin b^2 + \gamma\gamma' \sin c^2 + (\beta\gamma' + \gamma\beta')(\cos b \cos c - \cos a) \\ + (\gamma\alpha' + \alpha\gamma')(\cos c \cos a - \cos b) + (\alpha\beta' + \beta\alpha')(\cos a \cos b - \cos c) \\ \qquad = D \cos w, \end{array}\right.$$

in welcher α, β, γ die Kosinus der konkaven Winkel MOX, MOY, MOZ, ebenso α', β', γ' die Kosinus der konkaven Winkel $M'OX$, $M'OY$, $M'OZ$ sind, und D folgende Bedeutung hat:

$$(2)\qquad D = 1 - \cos a^2 - \cos b^2 - \cos c^2 + 2 \cos a \cos b \cos c.$$

Dieser bekannte Satz schließt den anderen ein, daß drei solche Richtungskosinus, wie α, β, γ, stets der Bedingung

$$(3)\quad \left\{\begin{array}{l} \alpha\alpha \sin a^2 + \beta\beta \sin b^2 + \gamma\gamma \sin c^2 + 2\,\beta\gamma\,(\cos b \cos c - \cos a) \\ + 2\,\gamma\alpha\,(\cos c \cos a - \cos b) + 2\,\alpha\beta\,(\cos a \cos b - \cos c) = D \end{array}\right.$$

Genüge leisten müssen.

Ist das Koordinatensystem rechtwinklig, so gehen die Gleichungen (1) und (3) in die beiden folgenden über:

$$\begin{aligned} \alpha\alpha' + \beta\beta' + \gamma\gamma' &= \cos w, \\ \alpha\alpha + \beta\beta + \gamma\gamma &= 1. \end{aligned}$$

Um daher auszudrücken, daß dann die drei Linien OM, OM', OM'' ein zweites rechtwinkliges Koordinatensystem bilden, sind folgende sechs Gleichungen nötig:

$$(4)\quad \left\{\begin{array}{llll} \alpha\alpha + \beta\beta + \gamma\gamma &= 1, & \alpha'\alpha'' + \beta'\beta'' + \gamma'\gamma'' &= 0, \\ \alpha'\alpha' + \beta'\beta' + \gamma'\gamma' &= 1, & \alpha''\alpha + \beta''\beta + \gamma''\gamma &= 0, \\ \alpha''\alpha'' + \beta''\beta'' + \gamma''\gamma'' &= 1, & \alpha\alpha' + \beta\beta' + \gamma\gamma' &= 0. \end{array}\right.$$

Sie sind auch hinreichend zu diesem Zwecke, wenn angenommen wird, daß das erste System rechtwinklig sei.

Der in der Überschrift angekündigte Satz besteht nun darin, daß diese letztere Beschränkung weggelassen werden darf, indem die Gleichungen (4) unzweifelhaft ausdrücken, daß beide Systeme durchaus rechtwinklig sein müssen. Der Beweis dieses merkwürdigen Theorems bildet den Gegenstand des gegenwärtigen Aufsatzes.

Zunächst mögen hier ohne weiteren Beweis die bekannten Folgerungen aus den Gleichungen (4) Platz finden, nämlich:

$$(5)\quad \begin{cases} \alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' = 1, & \beta\gamma + \beta'\gamma' + \beta''\gamma'' = 0, \\ \beta\beta + \beta'\beta' + \beta''\beta'' = 1, & \gamma\alpha + \gamma'\alpha' + \gamma''\alpha'' = 0, \\ \gamma\gamma + \gamma'\gamma' + \gamma''\gamma'' = 1, & \alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0, \end{cases}$$

und

$$(6)\quad \begin{cases} \beta'\gamma'' - \beta''\gamma' = \varepsilon\alpha, & \gamma'\alpha'' - \gamma''\alpha' = \varepsilon\beta, & \alpha'\beta'' - \alpha''\beta' = \varepsilon\gamma, \\ \beta''\gamma - \beta\gamma'' = \varepsilon\alpha', & \gamma''\alpha - \gamma\alpha'' = \varepsilon\beta', & \alpha''\beta - \alpha\beta'' = \varepsilon\gamma', \\ \beta\gamma' - \beta'\gamma = \varepsilon\alpha'', & \gamma\alpha' - \gamma'\alpha = \varepsilon\beta'', & \alpha\beta' - \alpha'\beta = \varepsilon\gamma'', \end{cases}$$

wo bekanntlich $\varepsilon\varepsilon = 1$ ist.

Die ternäre quadratische Form

$$F \equiv xx + yy + zz + 2\,yz\cos a + 2\,zx\cos b + 2\,xy\cos c,$$

[welche bekanntlich das Quadrat der Entfernung eines beliebigen Punktes (xyz) von dem Nullpunkte O des Koordinatensystems $OXYZ$ ausdrückt] hat zur Determinante den oben (2) mit D bezeichneten Ausdruck (das Quadrat des Volumens des von den drei Achsen $OX = OY = OZ = 1$ als Kanten gebildeten Parallelepipedums) und zur adjungierten Form:

$$F_1 \equiv xx\sin a^2 + yy\sin b^2 + zz\sin c^2 + 2\,yz(\cos b\cos c - \cos a) + 2\,zx(\cos c\cos a - \cos b) + 2\,xy(\cos a\cos b - \cos c).$$

Es ist dann bekanntlich die Determinante von F_1 das Quadrat der von F, also $= DD$, und die adjungierte Form F_2 von F_1 ist $\equiv DF$.

Wenn man folgende Bezeichnung einführt:

$$xx'\sin a^2 + yy'\sin b^2 + zz'\sin c^2 + (yz' + zy')\cos b\cos c - \cos a) + (zx' + xz')(\cos c\cos a - \cos b) + (xy' + yx')(\cos a\cos b - \cos c) \equiv F_1\begin{pmatrix} x, & y, & z \\ x', & y', & z' \end{pmatrix},$$

so ist aus der Theorie der ternären Formen weiter bekannt, daß

$$F_1\begin{pmatrix} x, & y, & z \\ x, & y, & z \end{pmatrix} F_1\begin{pmatrix} x', & y', & z' \\ x', & y', & z' \end{pmatrix} - \left[F_1\begin{pmatrix} x, & y, & z \\ x', & y', & z' \end{pmatrix}\right]^2$$
$$\equiv F_2\begin{pmatrix} yz'-zy', & zx'-xz', & xy'-yx' \\ yz'-zy', & zx'-xz', & xy'-yx' \end{pmatrix},$$

also im gegenwärtigen Falle

$$\equiv D\cdot F\begin{pmatrix} yz'-zy', & zx'-xz', & xy'-yx' \\ yz'-zy', & zx'-xz', & xy'-yx' \end{pmatrix} \tag{7}$$

ist.

Nach diesen Vorbemerkungen ist es nun leicht, den obigen Satz zu beweisen. $OXYZ$ sei das eine Koordinatensystem mit den Winkeln a, b, c; $OMM'M''$ das andere mit den Winkeln m, m', m''. OM bilde mit den drei Achsen OX, OY, OZ Winkel, deren Kosinus α, β, γ usw sind. Dann finden folgende sechs Gleichungen Statt:

$$\begin{cases} F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha, & \beta, & \gamma \end{pmatrix} = D, & F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha', & \beta', & \gamma' \end{pmatrix} = D, \\ F_1\begin{pmatrix} \alpha'', & \beta'', & \gamma'' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix} = D, & F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix} = D\cos m, \\ F_1\begin{pmatrix} \alpha'', & \beta'', & \gamma'' \\ \alpha, & \beta, & \gamma \end{pmatrix} = D\cos m', & F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \end{pmatrix} = D\cos m'', \end{cases} \tag{8}$$

welche allgemein die Beziehung zwischen irgend zwei dreiachsigen Koordinatensystemen ausdrücken. Wenn nun aber außerdem die Gleichungen (4), und folglich auch die (5) und (6) gelten, so erhält man durch Addition der drei ersten Gleichungen in (8):

$$\sin a^2 + \sin b^2 + \sin c^2 = 3D. \tag{9}$$

Ferner ergibt sich aus dem in (7) enthaltenen Theorem:

$$F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha, & \beta, & \gamma \end{pmatrix} F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha', & \beta', & \gamma' \end{pmatrix} - \left[F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \end{pmatrix}\right]^2$$
$$\equiv D\cdot F\begin{pmatrix} \beta\gamma'-\beta'\gamma, & \gamma\alpha'-\gamma'\alpha, & \alpha\beta'-\alpha'\beta \\ \beta\gamma'-\beta'\gamma, & \gamma\alpha'-\gamma'\alpha, & \alpha\beta'-\alpha'\beta \end{pmatrix} = D\cdot F\begin{pmatrix} \varepsilon\alpha'', & \varepsilon\beta'', & \varepsilon\gamma'' \\ \varepsilon\alpha'', & \varepsilon\beta'', & \varepsilon\gamma'' \end{pmatrix}$$

oder

$$DD - DD\cos m''^2$$
$$= D(\alpha''\alpha'' + \beta''\beta'' + \gamma''\gamma'' + 2\beta''\gamma''\cos a + 2\gamma''\alpha''\cos b + 2\alpha''\beta''\cos c),$$

also

$$D\sin m^2 = 1 + 2\beta\gamma\cos a + 2\gamma\alpha\cos b + 2\alpha\beta\cos c,$$
$$D\sin m'^2 = 1 + 2\beta'\gamma'\cos a + 2\gamma'\alpha'\cos b + 2\alpha'\beta'\cos c,$$
$$D\sin m''^2 = 1 + 2\beta''\gamma''\cos a + 2\gamma''\alpha''\cos b + 2\alpha''\beta''\cos c,$$

und hieraus durch Addition:

$$D(\sin m + \sin m'^2 + \sin m''^2) = 3.$$

Vergleicht man diese Relation mit der in (9) enthaltenen, so ergibt sich

$$(\sin a^2 + \sin b^2 + \sin c^2)(\sin m^2 + \sin m'^2 + \sin m''^2) = 3 \cdot 3,$$

und hieraus

$$\sin a^2 = \sin b^2 = \sin c^2 = \sin m^2 = \sin m'^2 = \sin m''^2 = 1;$$

d. h. alle sechs Koordinatenwinkel müssen rechte Winkel sein.

Bei diesem Beweis wurde natürlich vorausgesetzt, daß D von Null verschieden sei, d. h. daß OX, OY, OZ nicht in einer Ebene enthalten sind.

Göttingen, 15. Juli 1854.

IV.

Bemerkungen zu einer Aufgabe der Wahrscheinlichkeitsrechnung.

[Journal für reine und angewandte Mathematik, Bd. 50, S. 268—271 (1855)].

In einem der früheren Hefte des „Philosophical Magazine“ für 1854 hat G. Boole eine von A. Cayley gegebene Auflösung einer Wahrscheinlichkeitsaufgabe angegriffen. Wiewohl nicht zu zweifeln ist, daß der in diesem Angriff enthaltene Irrtum auch von anderen schon erkannt sei, so kommen doch die folgenden Bemerkungen denen, welche sich für diese schöne Theorie interessieren, vielleicht nicht unerwünscht.

Die Aufgabe lautet: Gegeben ist die Wahrscheinlichkeit α, daß eine Ursache A (welche ein gewisses Ereignis hervorbringen kann) zur Wirkung kommt, und die Wahrscheinlichkeit p, daß, wenn A wirkt, das Ereignis eintritt; ebenso die Wahrscheinlichkeit β, daß eine Ursache B zur Wirkung gelangt, und die Wahrscheinlichkeit q, daß, wenn B wirkt, das Ereignis eintritt: gesucht wird die Wahrscheinlichkeit u des Ereignisses, unter der Annahme, daß dasselbe von keiner anderen Ursache als von A und B hervorgebracht werden kann.

Cayley löset die Aufgabe auf folgende Weise: Es sei λ die Wahrscheinlichkeit, daß, wenn A wirkt, das Ereignis auch durch A hervorgebracht wird; μ die Wahrscheinlichkeit, daß, wenn B wirkt, das Ereignis auch durch B hervorgebracht wird; dann ist

$$p = \lambda + (1 - \lambda)\mu\beta, \quad q = \mu + (1 - \mu)\lambda\alpha.$$

Hieraus werden λ, μ bestimmt; und die gesuchte Wahrscheinlichkeit ist

$$u = \lambda\alpha + \mu\beta - \lambda\mu\alpha\beta.$$

Nachdem nun Boole diese Auflösung bei mehreren Spezialisierungen als richtig bewährt fand, sucht er nachzuweisen, daß sie

in dem Falle $p = 1$, $q = 0$ zu einem falschen Resultat führe. Er sagt: Es ist einleuchtend, daß die Wahrscheinlichkeit des Ereignisses in diesem Falle $= \alpha$ sein muß. Denn wenn die Ursache A das Ereignis stets hervorbringt, die Ursache B niemals, und das Eintreten des Ereignisses keiner anderen Ursache zugeschrieben werden kann, so muß die Wahrscheinlichkeit des „Ereignisses gleich der des Eintretens der Ursache A sein". Da sich gegen diesen Satz natürlich nichts einwenden läßt, und nun die Auflösung, wie sie Cayley darstellt, in diesem Falle entweder $u = 1$ oder $u = \alpha(1 - \beta)$ gibt, so schließt Boole, daß die ganze Auflösung fehlerhaft sein müsse, und gibt die Endformel seiner eigenen Auflösung, mit Hinzufügung besonderer Beschränkungen, aus denen sich allerdings für diesen Fall das gewünschte Resultat $u = \alpha$ ableiten läßt.

Man sieht indessen durchaus nicht, wo Cayley einen Fehler gemacht hätte; und in der Tat ist seine Auflösung auch (bis auf gewisse Beschränkungen, durch welche sie erst eindeutig gemacht werden muß) streng richtig, selbst in dem eben angeführten Falle; denn man findet leicht, daß $\alpha(1 - \beta)$ mit α übereinstimmt, indem α nichts anderes als Null sein kann. Wäre nämlich die Möglichkeit des Eintretens der Ursache A offen gelassen, d. h. wäre α nicht Null so könnte auch unmöglich die Wahrscheinlichkeit q des Ereignisses (unter der Annahme des Eintretens der Ursache B) gänzlich verschwinden, mag p noch so klein, nur nicht Null sein (in diesem Falle war aber $p = 1$ angenommen). Die gestellte Aufgabe ist daher widersinnig, wenn $q = 0$, α und p dagegen beide von Null verschieden angenommen werden. Dies ergibt sich auch durch einen Blick auf die Gleichungen von Cayley. Wenn man nämlich beachtet, daß μ, $(1 - \mu)$, λ, α, der Natur ihrer Bedeutung nach, nicht negativ sein können, so folgt aus der einen Gleichung $q = 0$, sowohl $\mu = 0$, als auch $\lambda\alpha = 0$, und die andere Gleichung geht in $p = \lambda$ über. Ist nun p von Null verschieden (es ist nicht nötig, daß p gerade $= 1$ sei), so muß auch $\alpha = 0$ sein; und die gesuchte Wahrscheinlichkeit u muß stets $= 0$ sein, mag q oder p, oder mögen beide $= 0$ sein; wie man es nicht anders erwarten darf.

Wenn nun aber dieser Vorwurf auch die obige Auflösung nicht trifft, so ist sie doch wenigstens noch unvollständig zu nennen, da die Bedingungen nicht angegeben sind, unter welchen die Aufgabe wirklich einen reellen Sinn hat, und da ferner zu entscheiden übrig

bleibt, welchen der beiden Werte von u, die den obigen Gleichungen genügen, man zu wählen habe. Dies soll hier geschehen.

Man verfährt mit der meisten Symmetrie, wenn man μ aus den Gleichungen für q und u, und ebenso λ aus den Gleichungen für p und u eliminiert. Dies gibt

$$(1) \qquad u - \beta q = (1-\beta)\lambda\alpha, \quad u - \alpha p = (1-\alpha)\mu\beta,$$

und wenn man diese Werte von $\lambda\alpha$, $\mu\beta$ in die Gleichung für u substituiert, so erhält man eine quadratische Gleichung, durch deren Auflösung sich

$$(2) \qquad u = \tfrac{1}{2}(1 - \alpha\beta + \alpha p + \beta q - \varrho)$$

ergibt, worin ϱ die noch zweideutige Quadratwurzel aus

$$\begin{aligned}\varrho\varrho = (1 - \alpha\beta + \alpha p + \beta q)^2 - 4(1-\beta)\alpha p,\\ - 4(1-\alpha)\beta q - 4\alpha p \cdot \beta q\end{aligned}$$

ist. Damit aber die Aufgabe lösbar sei, ist nötig: zuerst, daß ϱ reell, und weiter, daß u (als eine Wahrscheinlichkeit) ein positiver echter Bruch sei. Aber auch dies ist noch nicht genügend; und darin liegt eigentlich das Hauptinteresse der ganzen Aufgabe. Sie würde immer noch ohne Sinn bleiben, wenn die Hilfswahrscheinlichkeiten λ, μ nicht ebenfalls zwischen den Grenzen 0 und 1 enthalten wären, und es ist klar, daß mit diesen letzten Bedingungen auch zugleich die ersten erfüllt werden müssen. Es kommt daher nur darauf an, die Bedingungen aufzustellen, welche ausdrücken, daß λ, μ nicht außerhalb der genannten Grenzen liegen. Dies ist leicht, da man die Werte λ, μ aus den Gleichungen (1) erhält, wenn man in ihnen für u den in (2) gefundenen Ausdruck substituiert. Bei dieser Untersuchung kommt man auf die folgenden Gleichungen:

$$\begin{aligned}\varrho\varrho &= (1 - 2\alpha + \alpha\beta + \alpha p - \beta q)^2 + 4\alpha(1-\alpha)(1-\beta)(1-p)\\ &= (1 - 2\beta + \alpha\beta - \alpha p + \beta q)^2 + 4\beta(1-\beta)(1-\alpha)(1-q)\\ &= (1 - \alpha\beta + \alpha p - \beta q)^2 - 4\alpha(1-\beta)(p - \beta q)\\ &= (1 - \alpha\beta - \alpha p + \beta q)^2 - 4\beta(1-\alpha)(q - \alpha p).\end{aligned}$$

Aus den beiden ersten Formen für $\varrho\varrho$ geht hervor, daß es keiner besonderen Bedingung für die Realität von ϱ bedarf. Setzt man aber die Formen in Verbindung mit den Forderungen für λ, μ, so ergibt sich, daß in dem Ausdrucke (2) für u stets die positive Quadratwurzel für ϱ genommen werden muß. Vergleicht man endlich die beiden letzten Formen für $\varrho\varrho$ mit den Forderungen für λ und μ, so

erhält man, als die einzigen notwendig erforderlichen, aber auch vollständig genügenden Bedingungen, daß die beiden Differenzen

$$p - \beta q \quad \text{und} \quad q - \alpha p \tag{3}$$

nicht negativ sein dürfen.

Wenn man also, um ein Beispiel zu der Aufgabe zu geben, für α, β, p, q vier beliebige Zahlen innerhalb der Grenzen 0 und 1 angenommen hat, so muß man erst untersuchen, ob sie den beiden Bedingungen in (3) Genüge leisten. Beiläufig bemerkt, kann man bei einer solchen willkürlichen Wahl ebensooft ein widersinniges Beispiel wie ein passendes treffen; denn der Wert des vierfachen Integrals $\int\int\int\int d\alpha\, d\beta\, dp\, dq$ ist $= 1$, wenn man die Integrationen über alle Werte der Veränderlichen zwischen 0 und 1 ausdehnt; dagegen $= \frac{1}{2}$, wenn man diejenigen Werte ausschließt, welche den Bedingungen (3) nicht Genüge leisten. Man kann sich hiervon auch leicht durch geometrische Betrachtungen überzeugen.

In dem von Boole untersuchten Falle $q = 0$ reduzieren sich die Bedingungen (3) auf $\alpha p = 0$; dann wird $\varrho = 1 - \alpha\beta$, und folglich $u = 0$, ganz in Übereinstimmung mit den obigen Resultaten. Auch der Fall $\alpha = 0$ ist von Interesse. Dann ist $\varrho = 1 - \beta q$, und folglich $u = \beta q$ offenbar das richtige Resultat. Hierbei ist natürlich u von q unabhängig, und dennoch bleibt die Bedingung $p - \beta q \geqq 0$ in voller Kraft, und obgleich zur Bestimmung von u auf den Wert von p gar kein Gewicht fällt, so wäre es doch widersinnig, die Wahrscheinlichkeit p des Ereignisses unter der Annahme, daß die Ursache A zur Wirkung gelangt, kleiner als die Wahrscheinlichkeit βq anzunehmen, wenn auch diese Annahme durch die Bestimmung $\alpha = 0$ faktisch verboten ist. Und mit dieser Bemerkung, die, wie ich glaube, dazu geeignet ist, auf die Eigentümlichkeit dieser Art von Aufgaben ein frappantes Licht zu werfen, will ich meine Betrachtungen abbrechen.

Göttingen, 22. Juli 1854.

V.

Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 1—26 (1857)].

Es ist meine Absicht, dem in der Überschrift bezeichneten Gegenstand, welcher, von Gauß[*)] zuerst angeregt, später mit Erfolg von Galois, Serret, Schönemann[**)] wieder aufgenommen ist, eine einfache zusammenhängende Darstellung zu widmen, welche sich streng an die Analogie mit den Elementen der Zahlentheorie binden soll. Diese ist in der Tat so durchgreifend, daß es mit Ausnahme einiger unserem Gegenstand eigentümlicher Untersuchungen nur einer Wortänderung in den Beweisen der Zahlentheorie bedarf. Ich folge genau dem Gange, welchen Dirichlet in seinen Vorlesungen über die Zahlentheorie (oder in seiner kurzen Darstellung der Theorie der komplexen Zahlen im 24. Bande dieses Journals) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, daß ich meist nur die Hauptmomente der Beweise hervorhebe, da größere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müßte.

Die hier dargestellte Theorie, deren Erweiterungen auf der Hand liegen, ist vielfacher Anwendungen fähig, namentlich auf die Algebra, wie ich in einer späteren Abhandlung zeigen werde; zunächst schien es mir zweckmäßig, dieselbe ohne alle Einmischung algebraischer Prinzipien abzuhandeln.

Gebiet der Untersuchung; Definitionen und Fundamentalsätze.

1.

Unter einer Funktion einer Variabeln x wird hier immer eine ganze rationale Funktion von x verstanden, deren Koeffizienten reelle ganze Zahlen sind. Es werden die Eigenschaften solcher Funktionen

[*) Man vgl. C. F. Gauß' Werke, Bd. 2, S. 212—240.]

[**) E. Galois: Oeuvres mathématiques, S. 15—23. I. A. Serret: Cours d'algèbre, 2. Ausg., S. 343—370. Th. Schönemann, Journ. f. Math., Bd. 31, S. 269—325 und Bd. 32, S. 93—105, 1846.]

untersucht in bezug auf einen Modulus, der eine reelle Primzahl p ist. Zwei Funktionen A, B heißen kongruent in bezug auf den Modul p, in Zeichen

$$A \equiv B \pmod{p},$$

wenn sämtliche Koeffizienten der nach Potenzen von x geordneten Differenz $A - B$ durch p teilbar sind, oder, was dasselbe sagt, wenn die Koeffizienten gleich hoher Potenzen von x in den beiden Funktionen paarweise einander kongruent sind in bezug auf den Modulus p. Es ist daher diese Kongruenz nur ein Ausdruck für die Identität

$$A = B + p \cdot C,$$

in welcher C eine beliebige Funktion bedeutet. Hieraus gehen sogleich die beiden folgenden Sätze hervor:

Man darf in jeder Kongruenz zwischen zwei Funktionen die Variabeln x durch eine beliebige Funktion von x ersetzen.

Man darf jede Kongruenz beliebig oft nach der Variabeln x differentiieren.

Ebenso leuchten folgende Sätze ein, in welchen der Modulus p unveränderlich beibehalten wird:

Ist $A \equiv A'$, $B \equiv B'$, so ist auch $A \pm B \equiv A' \pm B'$, ferner $AB \equiv A'B'$, ferner $A^n \equiv A'^n$, wo n eine positive ganze Zahl bedeutet; und allgemein: Sind die beiden Seiten einer Kongruenz ganze rationale Funktionen (mit ganzen Zahlkoeffizienten) von einer Reihe von Funktionen A, B, C etc. der Variabeln x, so darf man dieselben (an beliebigen Stellen) durch ihnen resp. kongruente Funktionen A' B', C' etc. ersetzen.

2.

Der Exponent der höchsten Potenz von x in einer Funktion, deren Koeffizient nicht durch den Modul teilbar ist, heiße der Grad der Funktion. Aus dieser Definition, welche für alle Funktionen gilt, die nicht $\equiv 0 \pmod{p}$ sind, ergibt sich, daß alle die unendlich vielen einander kongruenten Funktionen einen und denselben Grad haben. Ist ferner α der Grad von A, β der Grad von B, so ist $\alpha + \beta$ der Grad von AB; denn das Produkt zweier durch eine Primzahl p nicht teilbaren Zahlen-Koeffizienten ist ebenfalls nicht teilbar

durch p. Hieraus folgt weiter: Ist $AB \equiv 0 \pmod{p}$, so ist mindestens eine der beiden Funktionen A, $B \equiv 0 \pmod{p}$; und ferner: Ist $AB \equiv A'B'$, und $A \equiv A'$ nicht $\equiv 0 \pmod{p}$, so ist $B \equiv B' \pmod{p}$; denn es ist $AB \equiv AB'$, oder $A(B - B') \equiv 0 \pmod{p}$. Dieser Satz gibt daher die Bedingung für die Berechtigung zur Division einer Kongruenz durch eine andere. Ferner ist leicht zu sehen, daß die Anzahl der einander nicht kongruenten (inkongruenten) Funktionen vom Grade α gleich $(p-1)p^{\alpha}$ ist; denn der Koeffizient von x^{α} kann $p-1$, der jeder niedrigeren Potenz kann p nach dem Modul p inkongruente Werte haben, und der Koeffizient jeder höheren Potenz ist $\equiv 0 \pmod{p}$. Dies Resultat gilt auch für den Fall $\alpha = 0$, insofern bei den Funktionen, welche $\equiv 0$ sind, überhaupt von einem Grade keine Rede ist.

3.

Sind A, B, C drei solche Funktionen von x, daß $A \equiv BC \pmod{p}$, so heißen B, C (oder alle diesen kongruente Funktionen) Divisoren oder Faktoren von A (oder jeder mit A kongruenten Funktion) in bezug auf den Modul p. Gleichbedeutend sind die Ausdrücke: A ist ein Multiplum von B, C; oder: A ist teilbar durch B, C. Diese Teilbarkeit nach einem Modulus ist natürlich nicht mit der algebraischen Teilbarkeit zu verwechseln, obwohl aus der letzteren stets die erstere folgt. Offenbar kann der Grad eines Divisors B von A nicht höher sein als der Grad von A. Jede Funktion ist teilbar durch jede der $p-1$ inkongruenten Funktionen vom Grade Null; denn jede der letzteren ist einer durch p nicht teilbaren Zahl a kongruent; bestimmt man nun a' so, daß $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, wo A jede beliebige Funktion bedeutet. Außer diesen $p-1$ Funktionen vom Grade Null hat keine andere die Eigenschaft, Divisor von jeder beliebigen Funktion zu sein; denn eine Funktion, deren Grad höher als Null ist, kann nicht mehr Divisor der Funktionen vom Grade Null sein. Man kann deshalb (zufolge der Analogie mit ähnlichen Untersuchungen) diese $p-1$ inkongruenten Funktionenklassen vom Grade Null Einheiten nennen.

Man kann jede Funktion vom Grade α kongruent setzen dem Produkte aus einer bestimmten Funktion vom Grade Null und einer Funktion vom Grade α, in welcher der Koeffizient von $x^{\alpha} \equiv 1 \pmod{p}$ ist (solche Funktionen sollen primäre heißen); denn ist a der durch

p nicht teilbare Koeffizient von x^α in A, und $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, worin $a'A$ eine primäre Funktion ist. — Die Anzahl der inkongruenten primären Funktionen vom Grade α ist gleich p^α.

Aus der Definition der Multipla ergeben sich unmittelbar die beiden folgenden Sätze: Ist eine Funktion ein Multiplum von einer zweiten, diese ein Multiplum von einer dritten, diese von einer vierten usw., so ist jede frühere in der Reihe dieser Funktionen ein Multiplum von jeder späteren. — Die Summe und die Differenz zweier Multipla von einer Funktion sind selbst wieder Multipla derselben Funktion.

4.

Von großer Bedeutung für die späteren Untersuchungen ist folgende Aufgabe: Zu untersuchen, ob zwei gegebene Funktionen A, A' nach dem Modul p gemeinschaftliche Divisoren haben.

Zunächst läßt sich zeigen, daß man stets eine Kongruenz von der Form

$$A \equiv QA' + A'' \pmod{p}$$

aufstellen kann, in welcher Q, A'' zwei neue Funktionen sind, deren letztere A'' einen niedrigeren Grad als A' hat, oder gar $\equiv 0 \pmod{p}$ ist. Denn es sei α der Grad von A, α' der von A'; im Falle nun $\alpha < \alpha'$ ist, braucht man nur $Q \equiv 0$, $A'' \equiv A \pmod{p}$ zu setzen; ist aber $\alpha \geqq \alpha'$, so kann man die Zahl q so bestimmen, daß $A - qx^{\alpha-\alpha'} \cdot A'$ von niedrigerem Grade α_1 als α ist; ist dann α_1 auch $< \alpha'$, so ist das Ziel schon erreicht, wenn man $Q \equiv qx^{\alpha-\alpha'}$ setzt; ist aber $\alpha_1 \geqq \alpha'$, so verfährt man mit der Funktion $A - qx^{\alpha-\alpha'} \cdot A'$ ebenso, wie bei dem ersten Schritte mit A; man bestimmt q_1 so, daß $A - qx^{\alpha-\alpha'} \cdot A' - q_1 x^{\alpha_1-\alpha'} \cdot A'$ von niedrigerem Grade ist als α_1 u. s. f., bis man zu einer Funktion von niedrigerem Grade als α' gelangt, was nach einer endlichen Anzahl von Operationen geschehen muß. Man setzt dann

$$Q \equiv qx^{\alpha-\alpha'} + q_1 x^{\alpha_1-\alpha'} + \text{etc.} \pmod{p},$$

und dann ist $A'' \equiv A - QA'$ von niedrigerem Grade als α'. W. Z. B. W.

Aus der so gebildeten Kongruenz folgt nun unmittelbar, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von A'', und umgekehrt, daß jeder gemeinschaftliche Divisor von A', A'' auch

Divisor von A sein muß. Man braucht daher die Operation nur fortzusetzen und ein System von Kongruenzen zu bilden:

$$\left.\begin{aligned} A &\equiv QA' + A'' \\ A' &\equiv Q'A'' + A''' \\ &\cdots\cdots\cdots \\ A^{(\nu-2)} &\equiv Q^{(\nu-2)}A^{(\nu-1)} + A^{(\nu)} \\ A^{(\nu-1)} &\equiv Q^{(\nu-1)}A^{(\nu)} \end{aligned}\right\} \text{(mod. } p\text{)},$$

in welchem die Grade α', α'' etc. eine abnehmende Reihe bilden, woraus von selbst folgt, daß nach einer endlichen Anzahl von Operationen es geschehen muß, daß eine Funktion $A^{(\nu-1)}$ durch die nächstfolgende $A^{(\nu)}$ teilbar ist. Schreitet man von der ersten bis zur letzten Kongruenz fort, so ergibt sich, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von $A^{(\nu)}$ sein muß; verfolgt man den umgekehrten Weg, so ergibt sich, daß $A^{(\nu)}$ Divisor aller vorhergehenden Funktionen und folglich auch gemeinschaftlicher Divisor der beiden Funktionen A, A' ist. Es heiße daher $A^{(\nu)}$ ein größter gemeinschaftlicher Divisor von A, A'. Multipliziert man $A^{(\nu)}$ mit einer beliebigen Funktion vom Grade Null (mit einer Einheit), so hat das Produkt offenbar dieselbe Eigenschaft wie $A^{(\nu)}$; es gibt daher $p-1$ inkongruente größte gemeinschaftliche Divisoren desselben Grades, und ein einziger unter diesen ist primär.

Drückt man vermöge der vorletzten Kongruenz $A^{(\nu)}$ durch $A^{(\nu-1)}$ und $A^{(\nu-2)}$, diese vermöge der vorhergehenden Kongruenzen durch die vorhergehenden Funktionen aus, so kommt man zuletzt auf eine Kongruenz von der Form

$$G \cdot A + G' \cdot A' \equiv A^{(\nu)} \text{ (mod. } p\text{)},$$

welche also stets möglich ist, wenn $A^{(\nu)}$ größter gemeinschaftlicher Divisor von A, A' ist.

5.

Ist der größte gemeinschaftliche Divisor $A^{(\nu)}$ der Funktionen A, A' vom Grade Null (also $\equiv 1$ (mod. p), wenn er primär ist), so heißen A, A' relativ prim gegeneinander.

Aus dieser Definition folgt der Hauptsatz: Sind A, A' zwei relative Primfunktionen, und ist M eine beliebige Funktion, so ist jeder gemeinschaftliche Divisor der beiden Funktionen AM, A' zugleich gemeinschaftlicher Divisor von M, A'. Denn multipliziert man

die Reihe der Kongruenzen, durch welche die Funktionen A, A', $A'', \cdots, A^{(\nu)}$ zusammenhängen, mit M, so ergibt sich unmittelbar, daß jeder gemeinschaftliche Divisor von AM, A' auch Divisor von $A''M$, $A'''M, \cdots, A^{(\nu)}M$ und folglich auch (da der Annahme nach $A^{(\nu)}$ vom Grade Null ist) von M, also gemeinschaftlicher Divisor von M, A' ist. (Dies folgt auch unmittelbar aus der Kongruenz $GAM + G'MA' \equiv A^{(\nu)}M$.)

Die wichtigsten Spezialfälle dieses Satzes sind die folgenden: Ist auch M relativ prim gegen A', so ist der größte gemeinschaftliche Divisor von M und A', und folglich auch der von AM und A' eine Funktion vom Grade Null, d. h. AM und A' sind relativ prim gegeneinander; und hieraus ergibt sich der Satz: Wenn zwei Reihen von Funktionen so beschaffen sind, daß jede Funktion der einen Reihe relativ prim gegen jede Funktion der anderen Reihe ist, so ist das Produkt aus sämtlichen Funktionen der einen Reihe relativ prim gegen das Produkt aus sämtlichen Funktionen der anderen Reihe.

Eine zweite Spezialisierung ist die folgende. Ist wieder A relativ prim gegen A', und ist AM durch A' teilbar, so ist A' als gemeinschaftlicher Divisor von AM, A' auch gemeinschaftlicher Divisor von M, A', also Divisor von M.

Hieraus folgt weiter: Ist jede der Funktionen A, B, C etc. relativ prim gegen jede der anderen, und ist ferner eine Funktion M durch jede der Funktionen A, B, C etc. teilbar, so ist M auch durch das Produkt $ABC\cdots$ teilbar. Denn der Annahme nach ist $M \equiv GA$ durch B teilbar, folglich ist, da A relativ prim gegen B ist, $G \equiv HB$, also $M \equiv HAB$ usw.

6.

Eine Funktion, welche nach dem Modul p nur solche Divisoren hat, die entweder ihr selbst oder Funktionen vom Grade Null (d. h. Einheiten) oder Produkten aus beiden kongruent sind (denn jede Funktion hat alle diese Divisoren), heißt (irreduktibel oder) eine Primfunktion nach dem Modul p; jede andere heißt (reduktibel oder) zusammengesetzt. Es leuchtet ein, daß eine beliebige Funktion entweder durch eine bestimmte Primfunktion teilbar, oder relativ prim gegen dieselbe ist. Ist daher ein Produkt AB durch eine Primfunktion P teilbar, so ist mindestens einer der Faktoren A, B für sich allein durch P teilbar; denn ist A nicht durch P

Sind endlich A, A' kongruent nach dem Modul M, und beide von niedrigerem Grade als M, so müssen A, A' auch nach dem einfachen Modul p einander kongruent sein.

8.

Man kann nun ein System von Funktionen aufstellen, so daß irgend eine beliebige Funktion einer von diesen Funktionen, aber auch nur einer einzigen nach dem Modulus M kongruent ist. Es sei A eine beliebige Funktion, so kann man, wie früher gezeigt ist, stets eine Kongruenz von der Form

$$A \equiv QM + A' \pmod{p}$$

aufstellen, in welcher A' von niedrigerem Grade ist als M. Stellt man daher sämtliche nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auf, so ist jede beliebige Funktion einer von diesen nach dem Modulus M kongruent, aber auch nur einer einzigen von ihnen, weil zwei nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auch in bezug auf M inkongruent sind. Ist μ der Grad von M, so ist p^μ die Anzahl dieser Funktionen, welche also ein System der verlangten Art bilden. Jedes solche System heiße ein **vollständiges System inkongruenter Funktionen in bezug auf den Modul M.** Multipliziert man jedes Glied eines solchen Systems mit einer und derselben Funktion, welche gegen den Modulus M relativ prim ist, so bilden die Produkte wieder ein solches System, wie sich leicht beweisen läßt.

9.

Seien N, N' etc. beliebige Funktionen, deren erste durch den Modulus M nicht teilbar ist, ferner n eine positive ganze Zahl, so heißt die Bedingung

$$Ny^n + N'y^{n-1} + \text{etc.} + N^{(n)} \equiv 0 \pmod{M}$$

eine **Kongruenz vom Grade n mit einer Unbekannten y**; und jede Funktion, welche für y substituiert diese Bedingung befriedigt, heißt eine **Wurzel** derselben. Ist eine solche Wurzel gefunden, so ist jede mit ihr nach dem Modul M kongruente Funktion ebenfalls eine Wurzel; die Hauptaufgabe ist daher, sämtliche nach dem Modul M inkongruente Wurzeln zu finden.

Wir betrachten zunächst die Kongruenz ersten Grades, welche auf die Form

$$Ay \equiv B \pmod{M}$$

gebracht werden kann. Nehmen wir zuerst an, A sei relativ prim gegen den Modul M, so gibt es (zufolge der Schlußbemerkung des vorigen Artikels) in jedem vollständigen System inkongruenter Funktionen eine, aber auch nur eine Funktion y, für welche $Ay \equiv B$ wird; die Kongruenz hat daher in diesem Falle nur eine einzige Wurzel (d. h. alle Wurzeln sind dieser einen nach M kongruent). Hat aber A mit M den größten gemeinschaftlichen Divisor D, so muß, wenn die Kongruenz lösbar sein soll, auch B durch D teilbar sein; in diesem Falle sei $A \equiv A'D$, $B \equiv B'D$, $M \equiv M'D \pmod{p}$, so folgt aus der obigen Kongruenz

$$A'y \equiv B' \pmod{M'}$$

und umgekehrt jene aus dieser. Da nun hierin A' relativ prim gegen den Modulus M', so hat die letztere Kongruenz eine, aber auch nur eine einzige Wurzel W nach dem Modulus M'. Alle Wurzeln der ersten Kongruenz sind daher in der Form

$$y \equiv W + HM' \pmod{p}$$

enthalten, und alle in dieser Form enthaltenen Funktionen y sind auch Wurzeln der ersten Kongruenz; und zwei in dieser Form enthaltene Funktionen $W + HM'$, $W + GM'$ sind stets, aber auch nur dann nach dem Modulus M inkongruent, wenn H und G nach dem Modulus D inkongruent sind. Mithin hat in diesem Falle die erste Kongruenz ebensoviel nach M inkongruente Wurzeln, als es nach dem Modul D inkongruente Funktionen gibt, also p^δ, wenn δ der Grad von D ist.

Für die späteren Untersuchungen ist auch noch die Lösung der folgenden Aufgabe wichtig: Seien M, N relativ prim gegeneinander; es soll die allgemeine Form der Funktionen y gefunden werden, welche die beiden Kongruenzen $y \equiv A \pmod{M}$, $y \equiv B \pmod{N}$ befriedigen. Aus der ersten Form folgt $y \equiv A + zM \pmod{p}$, wo z eine beliebige Funktion ist, welche aber der Bedingung $A + zM \equiv B \pmod{N}$ genügen muß; diese Kongruenz hat nach dem Vorhergehenden eine einzige Wurzel nach dem Modul N, und es folgt daraus die allgemeine Lösung $y \equiv W \pmod{MN}$.

10.

Hat man ein vollständiges System inkongruenter Funktionen in bezug auf den Modul M aufgestellt, so drängen sich die beiden folgenden Fragen auf: Wieviele dieser Funktionen haben mit M einen bestimmten Divisor D gemeinschaftlich? und: Wieviele unter diesen haben D zum größten gemeinschaftlichen Divisor mit M? — Die Beantwortung dieser Fragen ist unabhängig von der besonderen Wahl des vollständigen Systems inkongruenter Funktionen, da jede von zwei einander nach M kongruenten Funktionen denselben größten Divisor mit M gemeinschaftlich hat, wie die andere.

Die erste Frage ist im vorigen Artikel schon mit beantwortet; zwei Funktionen GD, HD sind stets, aber auch nur dann nach dem Modul $M \equiv ND$ inkongruent, wenn G, H nach dem Modul N inkongruent sind; ist daher ν der Grad von N, so gibt es $p^\nu = p^{\mu-\delta}$ nach M inkongruente Funktionen, welche mit M den Divisor D gemeinsam haben.

Irgend eine dieser Funktionen GD hat ferner stets, aber auch nur dann D zum größten gemeinschaftlichen Divisor mit M, wenn G relativ prim gegen N ist. Bezeichnen wir daher allgemein mit $\varphi(A)$ die Anzahl der in bezug auf A inkongruenten Funktionen, welche gegen A relativ prim sind, so ist die zweite von uns gesuchte Anzahl $= \varphi(N)$.

Schreiben wir nun sämtliche Divisoren von M auf, mit der Beschränkung, daß keiner von ihnen dem Produkt aus einem anderen in eine Einheit kongruent ist, also z. B. sämtliche inkongruente primäre Divisoren von M; so hat irgend eine Funktion einen dieser Divisoren, aber auch nur einen einzigen zum größten gemeinschaftlichen Divisor mit M, woraus in Verbindung mit dem Vorhergehenden der Satz

$$\Sigma\varphi(N) = p^\mu$$

folgt, wo das Summenzeichen sich auf ein so definiertes System von Divisoren N der Funktion M bezieht.

Aus diesem Satze ergibt sich sogleich der Ausdruck für $\varphi(M)$ in dem Falle, wenn M einer Potenz A^α einer einzigen Primfunktion kongruent ist. Ist α der Grad von A, so hat man zufolge des Satzes

$$\varphi(1) + \varphi(A) + \varphi(A^2) + \cdots + \varphi(A^{\alpha-1}) + \varphi(A^\alpha) = p^{\alpha\alpha},$$

und ebenso

$$\varphi(1) + \varphi(A) + \varphi(A^2) + \cdots + \varphi(A^{a-1}) = p^{\alpha(a-1)};$$

folglich

$$\varphi(A^a) = p^{\alpha a} - p^{\alpha(a-1)} = p^{\alpha a}\left(1 - \frac{1}{p^\alpha}\right).$$

Auf diesen Fall wird aber jeder andere durch folgenden Satz zurückgeführt: Sind M, N relativ prim gegeneinander, so ist $\varphi(MN) = \varphi(M)\varphi(N)$; welcher sich so beweisen läßt. Man bilde das vollständige System der gegen M relativ primen und nach M inkongruenten Funktionen G, deren Anzahl $\varphi(M)$; ebenso bilde man in bezug auf den Modulus N ein entsprechendes System von $\varphi(N)$ Funktionen H, und in bezug auf MN ein solches System von $\varphi(MN)$ Funktionen F. Es ergibt sich dann mit Hilfe der Schlußbemerkung des vorigen Artikels, daß allen $\varphi(M)\varphi(N)$ Kombinationen von Kongruenzen $y \equiv G \pmod{M}$ und $y \equiv H \pmod{N}$ eine, aber auch nur eine Lösung von der Form $y \equiv F \pmod{MN}$, und umgekehrt jeder der $\varphi(MN)$ Kongruenzen der letzteren Form eine, aber auch nur eine Kombination der ersteren Form entspricht; woraus unmittelbar $\varphi(MN) = \varphi(M)\varphi(N)$ folgt.

Seien nun A, B, C etc. sämtliche einander inkongruente Primfunktionen resp. von den Graden α, β, γ etc., welche in einer Funktion M vom Grade μ als Faktoren enthalten sind, und zwar so, daß keine dieser Primfunktionen etwa einem Produkt aus einer anderen von ihnen in eine Einheit kongruent ist, was man z. B. dadurch erreicht, daß man sie alle als primär annimmt; dann ist

$$\varphi(M) = p^\mu\left(1 - \frac{1}{p^\alpha}\right)\left(1 - \frac{1}{p^\beta}\right)\left(1 - \frac{1}{p^\gamma}\right)\cdots,$$

wie sich aus den vorhergehenden Sätzen leicht ergibt.

11.

Man schreibe das vollständige System der gegen M relativ primen und in bezug auf M inkongruenten Funktionen auf, deren Anzahl wir mit $\varphi(M)$ bezeichnet haben. Multipliziert man sie sämtlich mit einer und derselben F, welche sich in ihrem Komplex findet, so bilden die $\varphi(M)$ Produkte wieder ein solches System, so daß jedes Glied des einen Systems einem, aber auch nur einem einzigen Gliede des anderen Systems nach dem Modul M kongruent

ist. Multipliziert man daher alle diese $\varphi(M)$ Kongruenzen miteinander, und berücksichtigt, daß das Produkt der $\varphi(M)$ gegen M relativ primen Funktionen ebenfalls gegen M relativ prim ist, so erhält man den Satz

$$F^{\varphi(M)} \equiv 1 \pmod{M},$$

welcher dem verallgemeinerten Satze von Fermat in der Zahlentheorie entspricht.

Ist M eine Primfunktion P vom Grade π, so ist $\varphi(P) = p^\pi - 1$, und folglich

$$F^{p^\pi - 1} \equiv 1 \pmod{P},$$

wenn F eine durch P nicht teilbare Funktion bedeutet, und allgemein ist ohne alle Beschränkung für F

$$F^{p^\pi} \equiv F \pmod{P},$$

wie unmittelbar einleuchtet.

Hieraus folgt, daß die Auflösung der Kongruenz ersten Grades

$$Ay \equiv B \pmod{M}$$

in dem Falle, wo A gegen M relativ prim ist, durch die Formel

$$y \equiv BA^{\varphi(M)-1} \pmod{M}$$

gegeben wird.

12.

Von nun an wenden wir uns zu dem besonderen Falle, in welchem der Modulus der Kongruenzen eine Primfunktion P vom Grade π ist. Dann besteht folgender Satz: Eine Kongruenz $F(y) = Ny^n + N'y^{n-1} + \text{etc.} \equiv 0 \pmod{P}$ kann nicht mehr als n nach dem Modul P inkongruente Wurzeln haben. — Beweis: Wir nehmen an, der Satz sei für Kongruenzen vom Grade $n-1$ bewiesen, und zeigen, daß er dann auch für Kongruenzen vom Grade n gilt. Gesetzt dann, unsere Kongruenz $n$ten Grades hätte mehr als n inkongruente Wurzeln, also mindestens $n+1$. Sei W eine derselben, so ist für jede andere von dieser verschiedene y

$$F(y) - F(W) = (y - W)F_1(y) \equiv 0 \pmod{P},$$

wo $F_1(y)$ ein Polynom vom Grade $n-1$ ist, und folglich hätte, da $y - W$ nicht $\equiv 0 \pmod{P}$ sein kann, die Kongruenz $F_1(y) \equiv 0 \pmod{P}$ vom Grade $n-1$ gegen unsere Annahme mindestens n Wurzeln. — Nun ist der Satz für die Kongruenz ersten Grades schon früher bewiesen, folglich gilt er für jeden Grad.

Hat aber unsere Kongruenz $n$ten Grades wirklich n inkongruente Wurzeln W, W', W'' etc., so müssen die Koeffizienten gleich hoher Potenzen von y in den beiden Polynomen

$$F(y) = N y^n + N' y^{n-1} + \cdots,$$
$$G(y) = N(y - W)(y - W')(y - W'') \ldots$$

einander paarweise nach dem Modul P kongruent sein; denn sonst hätte die Kongruenz

$$F(y) - G(y) \equiv 0 \pmod{P},$$

deren Grad jedenfalls niedriger als n ist, n inkongruente Wurzeln sie darf daher gar keinen Grad haben, d. h. alle Koeffizienten derselben müssen durch P teilbar sein.

Nun haben wir im vorigen Artikel gesehen, daß die Kongruenz

$$y^{p^\pi - 1} \equiv 1 \pmod{P}$$

durch jede der $p^\pi - 1$ inkongruenten gegen P relativ primen Funktionen F befriedigt wird; mithin ist identisch

$$y^{p^\pi - 1} - 1 \equiv \Pi(y - F) \pmod{P},$$

wo $\Pi(y - F)$ das Produkt aus allen Faktoren $(y - F)$ bezeichnet Daraus folgt als Analogon zu dem Satze von Wilson in der Zahlentheorie das Theorem

$$\Pi(F) + 1 \equiv 0 \pmod{P},$$

wo $\Pi(F)$ das Produkt aus allen $p^\pi - 1$ nach P inkongruenten und durch P nicht teilbaren Funktionen bedeutet. Und umgekehrt muß P eine Primfunktion sein, wenn dieser Satz gilt; denn hätte P einen von einer Einheit verschiedenen Divisor D von niedrigerem Grade als π, so fände sich unter den $p^\pi - 1$ Funktionen F eine (im Art. 10 bestimmte) Anzahl solcher, welche mit P den Divisor D gemeinsam hätten; daraus würde aber folgen, daß auch die Einheit diesen Divisor hätte, was unmöglich ist.

Potenzreste.

13.

Sei M wieder ein beliebiger Modulus, A relativ prim gegen denselben, so sind auch alle Glieder der Reihe $1, A, A^2 \ldots$ in inf. relativ prim gegen M; es muß daher geschehen, daß $A^{m+n} \equiv A^m \pmod{M}$ und folglich $A^n \equiv 1 \pmod{M}$ wird. Sei a der kleinste

Wert von n, für welchen dies eintritt, so sagt man: A gehört zum Exponenten a; und es sind die a Funktionen

$$1, \quad A, \quad A^2, \quad \cdots, \quad A^{a-1}$$

inkongruent nach dem Modul M, woraus folgt, daß jede Zahl n, für welche $A^n \equiv 1 \pmod{M}$ wird, durch a teilbar ist. Zufolge des Art. 11 ist aber $A^{\varphi(M)} \equiv 1 \pmod{M}$, also ist a ein Divisor von $\varphi(M)$. Doch kann dies leicht direkt bewiesen werden, und daraus ergibt sich dann ein neuer Beweis des Satzes $A^{\varphi(M)} \equiv 1 \pmod{M}$. Man braucht zu dem Zwecke sich nur der bekannten Exhaustionsmethode zu bedienen, durch welche man die $\varphi(M)$ gegen M relativ primen Funktionen in $\frac{\varphi(M)}{a}$ Gruppen, jede von a Glieder zerfällt, deren allgemeine Form

$$F, \quad FA, \quad FA^2, \quad \cdots, \quad FA^{a-1}$$

ist, wo F irgend eine gegen M relativ prime Funktion bedeutet; denn es ist leicht zu zeigen, daß zwei solche Gruppen entweder ganz identisch oder ganz verschieden in bezug auf den Modulus M sind.

Wir verlassen den allgemeinen Fall und nehmen nun an, daß der Modulus eine Primfunktion P vom Grade π ist. Ist dann A irgend eine durch P nicht teilbare Funktion, welche in bezug auf P zum Exponenten a gehört, so ist a ein Divisor von $p^\pi - 1$; es fragt sich: gehören zu jedem Divisor a von $p^\pi - 1$ wirklich Funktionen A? und wieviele? —

Nehmen wir zuerst an, es gebe mindestens eine Funktion A, welche zu a gehört, so sind die a inkongruenten Funktionen $1, A, A^2, \cdots, A^{a-1}$ sämtliche Wurzeln der Kongruenz $y^a \equiv 1 \pmod{P}$; alle zum Exponenten a gehörenden Funktionen müssen daher Gliedern dieser Gruppe kongruent sein, und es ergibt sich leicht, daß eine Funktion $A^{a'}$ stets, aber auch nur dann zum Exponenten a gehört, wenn a' relativ prim gegen a ist. Wenden wir daher die Charakteristik φ in der Bedeutung an, wie sie in der Zahlentheorie gebräuchlich ist, so ist die Anzahl der zu einem Divisor a von $p^\pi - 1$ gehörenden Funktionen entweder $= 0$, oder $= \varphi a$. Da aber jede der $p^\pi - 1$ durch P nicht teilbaren Funktionen zu einem, aber auch nur zu einem einzigen der Divisoren $a, a', a'', \cdots$ von $p^\pi - 1$ gehören muß, und außerdem bekanntlich $\varphi a + \varphi a' + \varphi a'' + \cdots = p^\pi - 1$ ist, so ergibt sich leicht, daß zu jedem Divisor a von $p^\pi - 1$ wirklich φa Funktionen gehören.

Es gibt daher auch $\varphi(p^\pi - 1)$ inkongruente durch den Modul P nicht teilbare Funktionen, welche zum Exponenten $p^\pi - 1$ gehören. Sei G irgend eine derselben, so sind die $p^\pi - 1$ Funktionen

$$1,\ G,\ G^2,\ G^3,\ \cdots,\ G^{p^\pi - 2}$$

sämtlich inkongruent, und sie bilden daher das vollständige System der inkongruenten durch P nicht teilbaren Funktionen, so daß also jede durch P nicht teilbare Funktion einer von ihnen, aber auch nur einer einzigen kongruent ist. Diese $\varphi(p^\pi - 1)$ Funktionen G heißen primitive Wurzeln der Primfunktion P. Nimmt man eine derselben G als Basis an, und ist F eine beliebige durch P nicht teilbare Funktion, so kann man stets

$$F \equiv G^n \pmod{P}$$

setzen, wo $n = 0$ oder eine positive ganze Zahl $< p^\pi - 1$ ist. Diese Zahl n heißt dann der Index der Funktion F bezüglich der Basis G, in Zeichen

$$F \equiv G^{\text{Ind. } F} \pmod{P}.$$

Dann leuchten folgende Sätze ein, in welchen A, B Funktionen bedeuten, welche durch P nicht teilbar sind, und in denen die Basis der Indizes unverändert bleibt: Ind. $(AB) \equiv$ Ind. $A +$ Ind. B (mod. $p^\pi - 1$), Ind. $(A^n) \equiv n$ Ind. A (mod. $p^\pi - 1$); ferner folgt aus $A \equiv B$ (mod. P) notwendig Ind. $A =$ Ind. B und umgekehrt.

Ein anderer Satz, welcher seiner Natur nach von der Wahl der Basis unabhängig ist, lautet folgendermaßen: Gehört eine Funktion A zum Exponenten a, so ist $\frac{p^\pi - 1}{a}$ der größte gemeinschaftliche Divisor von $p^\pi - 1$ und Ind. A; und umgekehrt.

Binomische Kongruenzen.

14.

Soll die binomische Kongruenz $y^n \equiv A$ (mod. P), in welcher A eine durch P nicht teilbare Funktion bedeutet, lösbar sein, so muß n Ind. $y \equiv$ Ind. A (mod. $p^\pi - 1$) sein; ist nun δ der größte gemeinschaftliche Divisor von n und $p^\pi - 1$, so muß auch Ind. A durch δ teilbar sein, wenn diese Kongruenz möglich sein soll, und dann hat sie in der Tat δ nach dem Modul $p^\pi - 1$ inkongruente Wurzeln Ind. y, denen ebenso viele nach dem Modul P inkongruente Wurzeln y der binomischen Kongruenz entsprechen.

Die erforderliche und hinreichende Bedingung für die Möglichkeit dieser Kongruenz, daß nämlich Ind. A durch den größten gemeinschaftlichen Divisor δ von n und $p^\pi - 1$ teilbar sein muß, ist unabhängig von der Wahl der Basis und offenbar identisch mit der Bedingung, daß A eine Wurzel der Kongruenz $y^{\frac{p^\pi - 1}{\delta}} \equiv 1 \pmod{P}$ ist; und man hätte dieses Kriterium auch leicht ohne Hilfe der Theorie der Indizes ableiten können. Zugleich leuchtet nun ein, daß die vorgelegte binomische Kongruenz für $\frac{p^\pi - 1}{\delta}$ inkongruente Funktionen A möglich ist, und nur für diese.

Quadratische Reste.

15.

Wenden wir die letzten Resultate auf den Fall an, in welchem $n = 2$ und p ungerade ist (der Fall $p = 2$ ist leicht zu absolvieren), so ergibt sich, daß die Kongruenz

$$y^2 \equiv A \pmod{P}$$

stets, aber auch nur dann möglich ist, wenn A eine der $\frac{1}{2}(p^\pi - 1)$ Wurzeln der Kongruenz

$$y^{\frac{1}{2}(p^\pi - 1)} \equiv 1 \pmod{P}$$

ist, die wir quadratische Reste der Primfunktion P nennen während die übrigen $\frac{1}{2}(p^\pi - 1)$ inkongruenten durch P nicht teilbaren Funktionen quadratische Nichtreste von P heißen; und jedesmal, wenn A quadratischer Rest von P ist, hat die vorgelegte Kongruenz zwei inkongruente Wurzeln. Die $\frac{1}{2}(p^\pi - 1)$ Nichtreste sind offenbar die Wurzeln der Kongruenz

$$y^{\frac{1}{2}(p^\pi - 1)} \equiv -1 \pmod{P}.$$

Doch lassen sich alle diese Sätze auch unmittelbar aus den ersten Elementen ableiten, und zugleich ergeben sich dann neue Beweise für die beiden Sätze, welche denen von Fermat und Wilson in der Zahlentheorie analog sind. Ist A eine bestimmte, der $p^\pi - 1$ durch P nicht teilbaren Funktionen, so gehört zu jeder beliebigen F derselben eine, aber auch nur eine F', so daß $FF' \equiv A \pmod{P}$; wenn nun erstens A quadratischer Nichtrest von P ist (d. h. wenn die Kongruenz $y^2 \equiv A \pmod{P}$ unmöglich), so sind F und F' stets

inkongruent, und es zerfällt das System sämtlicher $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare F, F'; woraus leicht folgt, daß

$$\Pi(F) \equiv A^{\frac{1}{2}(p^\pi - 1)} \pmod{P}$$

ist, wo das Zeichen Π dieselbe Bedeutung hat, wie im Art. 12. Ist aber zweitens A quadratischer Rest, d. h. ist die Kongruenz $y^2 \equiv A \pmod{P}$ möglich, so ist einleuchtend, daß diese zwei Wurzeln von der Form W und $-W$ hat, und das Produkt dieser beiden Funktionen ist $\equiv -A \pmod{P}$; die übrigen $p^\pi - 3$ Funktionen F zerfallen aber, wie im ersten Falle, in $\frac{1}{2}(p^\pi - 3)$ Paare inkongruenter Funktionen F, F'; woraus folgt, daß in diesem Falle

$$\Pi(F) \equiv -A^{\frac{1}{2}(p^\pi - 1)} \pmod{P}$$

ist. Da nun 1 quadratischer Rest von P ist, so folgt aus dem zweiten Falle zunächst der Satz

$$\Pi(F) + 1 \equiv 0 \pmod{P},$$

sodann, daß

$$A^{\frac{1}{2}(p^\pi - 1)} \equiv +1 \text{ oder } \equiv -1 \pmod{P},$$

je nachdem A quadratischer Rest oder Nichtrest von P ist, und endlich, daß in beiden Fällen

$$A^{p^\pi - 1} \equiv 1 \pmod{P}$$

ist. Die Anzahl der quadratischen Reste bestimmt sich endlich folgendermaßen. Man kann die $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare von der Form F, $-F$ zerlegen, woraus folgt, daß es höchstens $\frac{1}{2}(p^\pi - 1)$ inkongruente Quadrate, also auch höchstens ebenso viel inkongruente quadratische Reste gibt; da aber außerdem je zwei verschiedenen Paaren, wie leicht zu beweisen ist, wirklich inkongruente Quadrate entsprechen, so gibt es in der Tat $\frac{1}{2}(p^\pi - 1)$ quadratische Reste und ebenso viele Nichtreste.

16.

Das Zeichen $\left(\frac{A}{P}\right)$ möge $+1$ oder -1 bedeuten, je nachdem (die durch die Primfunktion P nicht teilbare Funktion) A quadratischer Rest oder Nichtrest von P ist. Dann leuchten folgende Sätze ein:

1. Ist $A \equiv B \pmod{P}$, so ist $\left(\frac{A}{P}\right) = \left(\frac{B}{P}\right)$.

2. $\left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right)$ oder allgemeiner: das Produkt aus einer beliebigen Anzahl von Funktionen (die durch P nicht teilbar sind) ist quadratischer Rest oder Nichtrest, je nachdem die Anzahl der Faktoren, welche Nichtreste sind, gerade oder ungerade ist.

Man kann auch noch ein anderes Kriterium aufstellen, um zu entscheiden, ob eine Funktion A quadratischer Rest oder Nichtrest von P ist. Teilt man nämlich sämtliche $p^n - 1$ Funktionen F in $\frac{1}{2}(p^n - 1)$ Paare von der Form F, $-F$, und nimmt aus jedem Paare willkürlich eine Funktion, so erhält man eine Gruppe von $\frac{1}{2}(p^n - 1)$ Funktionen F, deren Quadrate sämtlich inkongruent sind, und ebenso bilden die übrigen $\frac{1}{2}(p^n - 1)$ Funktionen $-F$ eine solche Gruppe. Nun bilde man die Produkte aus jeder Funktion der einen Gruppe in die Funktion A und bezeichne mit μ die Anzahl derjenigen unter diesen Produkten, welche Funktionen der anderen Gruppe kongruent sind; so ist leicht zu zeigen, daß

$$A^{\frac{1}{2}(p^n-1)} \equiv (-1)^{\mu} \pmod{P}$$

oder $\left(\frac{A}{P}\right) = (-1)^{\mu}$ ist. Je nachdem also μ gerade oder ungerade, ist A quadratischer Rest oder Nichtrest von P.

17.

Die Frage: „Von welchen Primfunktionen P ist eine gegebene Funktion A quadratischer Rest?“, welche für die Theorie der quadratischen Formen (mit Funktionen einer Variablen x) von Wichtigkeit ist, wird vermöge des vorigen Artikels auf den Fall reduziert, in welchem A eine Primfunktion R (vom Grade ϱ) ist. Die analoge Frage in der Zahlentheorie wird bekanntlich durch den (zuerst von Gauß bewiesenen) sogenannten Reziprozitäts-Satz von Legendre beantwortet. Diese Analogie, welche sich bisher in allen Prinzipien und Beweisen bewährt hat, läßt keinen Zweifel an der Existenz eines entsprechenden Satzes in unserer Theorie übrig. Dieses Theorem lautet in der Tat

$$\left(\frac{P}{R}\right)\left(\frac{R}{P}\right) = \left(\frac{-1}{p}\right)^{n \cdot \varrho},$$

worin P, R primäre Primfunktionen resp. von den Graden π, ϱ bedeuten, und $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ das Zeichen von Legendre ist. Der Fall, in welchem P, R nicht primär sind, läßt sich unmittelbar auf diesen zurückführen. Denn bedeutet E irgend eine der $p-1$ Einheiten, so ist stets $\left(\frac{A}{EP}\right) = \left(\frac{A}{P}\right)$, wo A irgend eine durch P nicht teilbare Funktion ist; und außerdem ist $\left(\frac{E}{P}\right) = \left(\frac{e}{p}\right)^{\pi}$, wo e eine Zahl $\equiv E \pmod{p}$ und $\left(\frac{e}{p}\right)$ das Zeichen von Legendre ist. Beide Sätze sind leicht zu beweisen.

Der Beweis unseres Theorems kann ganz analog dem fünften Gaußschen für den Satz von Legendre geführt werden und stützt sich dann auf das am Schlusse des vorigen Artikels bewiesene Lemma. Man betrachtet die vollständigen Systeme inkongruenter Funktionen (mit Ausnahme derer, welche $\equiv 0$ sind) in bezug auf die drei Moduli P, R, PR, und wählt dazu immer die inkongruenten Funktionen, deren Grade kleiner sind als der des entsprechenden Moduls. Jedes dieser drei Systeme teilt man in zwei Gruppen von gleich viel Gliedern ein, deren erstere sämtliche Funktionen F enthält, deren höchster Koeffizient einer der Zahlen $1, 2, \cdots, \frac{1}{2}(p-1)$ kongruent ist, während die andere Gruppe die übrigen Funktionen $-F$ enthält, deren höchster Koeffizient einer der Zahlen $-1, -2, \cdots, -\frac{1}{2}(p-1)$ kongruent ist. Die weitere Einteilung der beiden Gruppen des dritten Systems, welches sich auf den Modulus PR bezieht, in jedesmal acht Klassen mit Bezug auf die Moduli P, R und die Schlußfolgerungen daraus bis zu dem letzten Resultat hin, in welchem der Beweis des Theorems enthalten ist, sind denen der zitierten Abhandlung von Gauß so ähnlich, daß die vollständige Durchführung Niemandem entgehen kann. Und hiermit wollen wir diesen Teil unserer Theorie verlassen, da seine weitere Entwicklung sich von selbst ergibt.

Bestimmung der Primfunktionen.

18.

Sei P eine Primfunktion vom Grade π, A eine beliebige Funktion; bildet man die unendliche Reihe A, A^p, A^{p^2}, A^{p^3}, $\cdots$, so muß es natürlich geschehen, daß ein Glied A^{p^m+n} einem früheren Gliede A^{p^m}

nach dem Modul P kongruent ist (im Falle A der Null oder einer Einheit kongruent ist, wird schon $A^p \equiv A \pmod{P}$); da ferner allgemein $A^{p^\pi} \equiv A \pmod{P}$ ist, so kann man annehmen, daß $m < \pi$ ist; erhebt man daher die Kongruenz $A^{p^{m+n}} \equiv A^{p^m}$ zur Potenz $p^{\pi-m}$, so ergibt sich leicht $A^{p^n} \equiv A \pmod{P}$. Sei nun $\varrho > 0$ der niedrigste Wert von n, für welchen dies eintritt, so wollen wir sagen: Die Funktion A paßt zur Zahl ϱ. Dann sind die ϱ Funktionen

$$(\mathfrak{A}.) \qquad A,\ A^p,\ A^{p^2},\ \ldots,\ A^{p^{\varrho-1}}$$

sämtlich inkongruent, denn aus $A^{p^{m+n}} \equiv A^{p^m}$ würde wieder $A^{p^n} \equiv A$ folgen. Daraus ergibt sich dann leicht, daß, wenn $A^{p^n} \equiv A$ ist, n notwendig durch ϱ teilbar sein muß. Also ist jedenfalls ϱ ein Divisor von π.

Es fragt sich nun: Passen zu jedem Divisor ϱ von π wirklich Funktionen? und wieviele? — Zunächst leuchtet ein, daß die Anzahl der (inkongruenten) Funktionen, welche zu ϱ passen, ein Multiplum $\varrho \cdot \psi(\varrho)$ von ϱ sein muß (die Null vorläufig nicht ausgeschlossen). Denn wenn A zu ϱ paßt, so passen auch die ϱ in dem Komplex ($\mathfrak{A}.$) enthaltenen Funktionen zu ϱ; ebenso die ϱ Funktionen

$$(\mathfrak{B}.) \qquad B,\ B^p,\ B^{p^2},\ \ldots,\ B^{p^{\varrho-1}},$$

wenn B zu ϱ paßt; und endlich sind zwei solche Komplexe ($\mathfrak{A}.$) und ($\mathfrak{B}.$) entweder ganz identisch, oder ganz verschieden in bezug auf den Modulus P.

Ferner ist klar, daß alle zu ϱ passenden Funktionen unter den Wurzeln der Kongruenz

$$y^{p^\varrho} \equiv y \pmod{P}$$

zu suchen sind, und jede Wurzel dieser Kongruenz paßt zu einem bestimmten Divisor von ϱ. Endlich hat diese Kongruenz in der Tat p^ϱ inkongruente Wurzeln, was sich unmittelbar daraus ergibt, daß $y^{p^\pi} - y$ algebraisch durch $y^{p^\varrho} - y$ teilbar ist. Und da unter diesen p^ϱ Wurzeln auch sämtliche Funktionen enthalten sind, die zu einem beliebigen Divisor δ von ϱ passen, so ergibt sich die Gleichung

$$\Sigma\delta \cdot \psi(\delta) = p^\varrho,$$

wo sich das Summenzeichen auf sämtliche Divisoren δ von ϱ bezieht. Stellt man nun diese Gleichung für jeden Divisor ϱ von π auf, so erhält man offenbar ebensoviel Gleichungen, als unbekannte Zahlen $\psi(\delta)$ zu bestimmen sind. Für den Fall, daß π eine Potenz a^α

einer Primzahl a ist, ergibt sich die Auflösung unmittelbar; denn dann ist, wenn α' eine der Zahlen 1, 2, 3, $\cdots$, α bedeutet,

$$1 \cdot \psi(1) + a \cdot \psi(a) + \cdots + a^{\alpha'} \cdot \psi(a^{\alpha'}) = p^{a^{\alpha'}},$$
$$1 \cdot \psi(1) + a \cdot \psi(a) + \cdots + a^{\alpha'-1} \psi(a^{\alpha'-1}) = p^{a^{\alpha'-1}},$$

folglich $a^{\alpha'} \cdot \psi(a^{\alpha'}) = p^{a^{\alpha'}} - p^{a^{\alpha'-1}}$ die Anzahl der inkongruenten Funktionen, welche zu dem Divisor $a^{\alpha'}$ von $\pi = a^{\alpha}$ passen.

Doch läßt sich auch die allgemeine Auflösung des Problems vermöge des folgenden allgemeinen Theorems leicht hinschreiben: Seien $f(m)$ und $F(m)$ zwei von der ganzen Zahl m in der Weise abhängige Funktionen, daß die letztere gleich ist der Summe der Werte der ersteren für alle Divisoren von m; so läßt sich umgekehrt $f(m)$ als algebraische Summe einer Reihe von Werten der Funktion $F(m)$ darstellen. Seien a, b, c, $\cdots$ sämtliche voneinander verschiedenen Primzahlen, welche in m aufgehen, so ist

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \Sigma F\left(\frac{m}{abc}\right) + \cdots,$$

wo die Summenzeichen auf der rechten Seite sich der Reihe nach auf alle Kombinationen zu 1, 2, 3 usw. aus den Primzahlen $a, b, c, \cdots$ beziehen. Und es ist leicht zu sehen, daß dasselbe Theorem auch gilt, wenn die Funktionen f, F sich auf irgendwelche Elemente m beziehen, denen jedesmal bestimmte andere Elemente nach denselben Prinzipien entsprechen, wie die Divisoren einer ganzen Zahl dieser Zahl selbst entsprechen.

So folgt aus diesem Satze unmittelbar die Bestimmung der in der Zahlentheorie gebräuchlichen Funktion

$$\varphi(m) = m - \Sigma\frac{m}{a} + \Sigma\frac{m}{ab} - \Sigma\frac{m}{abc} + \cdots$$
$$= m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots$$

aus dem Satze $\Sigma\varphi(\delta) = m$, wo δ alle Divisoren von m zu durchlaufen hat.

Ebenso ergibt sich aus dem in Art. 10 bewiesenen Satze $\Sigma\varphi(N) = p^{\mu}$ die Umkehrung

$$\varphi(M) = p^{\mu} - \Sigma p^{\mu-\alpha} + \Sigma p^{\mu-(\alpha+\beta)} - \Sigma p^{\mu-(\alpha+\beta+\gamma)} + \cdots$$
$$= p^{\mu}\left(1-\frac{1}{p^{\alpha}}\right)\left(1-\frac{1}{p^{\beta}}\right)\left(1-\frac{1}{p^{\gamma}}\right)\cdots;$$

denn in diesem Falle war $F(M) = p^{\mu}$.

In unserem Falle haben wir $f(m) = m \cdot \psi(m)$ und $F(m) = p^m$, und es ergibt sich also

$$m \cdot \psi(m) = p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots$$

als die Anzahl der nach dem Modul P inkongruenten Funktionen, welche zu dem Divisor m des Grades π von P passen; und hier bezeichnen wieder $a, b, c \cdots$ sämtliche voneinander verschiedene Primzahlen, welche in m aufgehen.

Die Unabhängigkeit dieses Ausdrucks von dem Multiplum π der Zahl m und der besonderen Natur der Primfunktion P läßt vermuten, daß derselbe eine allgemeinere Bedeutung hat, was sich auch bald herausstellen wird.

19.

Satz: Die Funktion $x^{p^\pi} - x$ ist nach dem Modul p kongruent dem Produkt aus allen primären inkongruenten Primfunktionen, deren Grade Divisoren von π sind. —

Beweis: 1. Die vorgelegte Funktion kann keine einander kongruenten Faktoren enthalten, da ihre Derivierte einer Einheit kongruent ist.

2. Sie ist durch jede Primfunktion R teilbar, deren Grad ϱ ein Divisor von π ist. Denn es ist $x^{p^\varrho} \equiv x \pmod{R}$, und wenn man beide Seiten immer wieder zur Potenz p^ϱ erhebt

$$x \equiv x^{p^\varrho} \equiv x^{p^{2\varrho}} \equiv \cdots \equiv x^{p^\pi} \pmod{R}.$$

3. Sie kann keinen Primfaktor von höherem Grade als π enthalten. Denn bezeichnet $f(x)$ eine beliebige Funktion, so ist, wie leicht zu zeigen, für jede positive ganze Zahl h:

$$f(x)^{p^h} \equiv f(x^{p^h}) \pmod{p}.$$

Ist nun Q irgend ein Primfaktor von $x^{p^\pi} - x$, so ist also

$$f(x)^{p^\pi} \equiv f(x^{p^\pi}) \equiv f(x) \pmod{Q};$$

mithin sind alle in bezug auf Q inkongruenten Funktionen $f(x)$ Wurzeln der Kongruenz $y^{p^\pi} \equiv y \pmod{Q}$, und folglich kann die Anzahl dieser in bezug auf Q inkongruenten Funktionen nicht größer als p^π, folglich der Grad von Q nicht größer als π sein.

4. Der Grad jedes Primfaktors von $x^{p^\pi} - x$ ist ein Divisor von π. Denn es folgt aus 3., daß die Funktion x in bezug auf eine Primfunktion Q vom Grade μ zur Zahl μ selbst paßt (so daß die μ

Funktionen $x, x^p, x^{p^2}, \cdots, x^{p^{\mu-1}}$ in bezug auf Q inkongruent sind); ist daher $x^{p^\pi} \equiv x \pmod{Q}$, so muß μ ein Divisor von π sein.

5. Die Funktion $x^{p^\pi} - x$ enthält daher alle Primfunktionen, deren Grade Divisoren von π sind, und nur solche, ferner jede nur einmal, und da ihr höchster Koeffizient $\equiv 1 \pmod{p}$ ist, so ist sie dem Produkt aus allen primären Primfunktionen kongruent, deren Grade Divisoren von π sind. W. z. b. w.

20.

Bezeichnet man daher die Anzahl der primären Primfunktionen von irgend einem Grade ϱ mit $\psi(\varrho)$, so ist

$$\Sigma \varrho \cdot \psi(\varrho) = p^\pi,$$

worin sich das Summenzeichen auf alle Divisoren ϱ der Zahl π bezieht. Vergleicht man diese Formel mit der im Art. 18, wo die allgemeine Auflösung solcher Gleichungen gelehrt ist, so ergibt sich, daß die Funktion ψ hier wie dort für gleiche Argumente stets denselben Wert hat; und es ist nun auch nicht schwer, die Identität der Bedeutung derselben in beiden Untersuchungen nachzuweisen.

Zunächst ziehen wir aus der im Art. 18 entwickelten Form für $m \cdot \psi(m)$ den Schluß, daß es in der Tat Primfunktionen von jedem Grade m gibt; denn wäre die rechte Seite $= 0$, so könnte man sie durch ihr letztes Glied $p^{\overset{m}{abc\cdots}}$ dividieren, woraus folgen würde, daß die Zahl 1 als algebraische Summe einer Reihe von Potenzen einer Primzahl $p(>1)$ darstellbar wäre, was unmöglich ist, da 1 nicht durch p teilbar ist; und negativ kann $m \cdot \psi(m)$ seiner Bedeutung nach nicht sein.

Sei nun P eine Primfunktion vom Grade π, und A eine Funktion, welche in bezug auf den Modulus P zu dem Divisor ϱ von π paßt. Dann sind die Koeffizienten sämtlicher Potenzen von y in dem Produkte

$$(y - A)(y - A^p)(y - A^{p^2}) \cdots (y - A^{p^{\varrho-1}})$$

nach dem Modulus P Zahlen kongruent. Denn jeder Koeffizient ist eine symmetrische Funktion der ϱ Funktionen $A, A^p, \cdots, A^{p^{\varrho-1}}$ und bleibt daher sich selbst kongruent, wenn man x durch x^p ersetzt, d. h. er ist eine Wurzel der Kongruenz $y^p \equiv y \pmod{P}$. Mit anderen Worten, diese Gruppe von ϱ Funktionen, welche zu dem

Divisor ϱ passen, bildet das vollständige Wurzelsystem einer Kongruenz

$$R(y) \equiv 0 \pmod{P}$$

vom Grade ϱ, deren Koeffizienten von x unabhängig sind. Umgekehrt läßt sich aber auch leicht zeigen, daß, wenn eine Kongruenz, deren Koeffizienten von x unabhängig sind, eine Wurzel A besitzt, welche zu dem Divisor ϱ von π paßt, sie auch die übrigen $\varrho - 1$ Funktionen A^p, A^{p^2}, ..., $A^{p^{\varrho-1}}$ zu Wurzeln haben muß (ein Satz, der sich leicht verallgemeinern läßt). Daraus folgt, daß $R(y)$ nach dem Modul p nicht in Faktoren niedrigen Grades zerlegt werden kann, oder, mit anderen Worten, daß $R(x)$ eine Primfunktion vom Grade ϱ ist. Die identische Kongruenz

$$y^{p^\pi} - y \equiv \Pi(y - F) \pmod{P}$$

führt daher, wenn man die Faktoren, welche eine Gruppe zusammengehöriger zu einer und derselben Zahl passender Funktionen F bilden, jedesmal in einen Faktor zusammenzieht, zur Zerlegung der Funktion $y^{p^\pi} - y$ in ihre irreduzibeln Faktoren in bezug auf den Modulus p. Auf diese Weise ist der Zusammenhang der Betrachtungen des Art. 18 mit der Bestimmung der Anzahl der Primfunktionen vollständig dargelegt.

21.

Sei nun M eine beliebige Funktion vom Grade μ, und zwar

$$M \equiv E A^a B^b C^c \cdots \pmod{p},$$

worin E eine Einheit, A, B, C etc. inkongruente primäre Primfunktionen resp. von den Graden α, β, γ etc. sind. Sei ferner π irgend eine durch sämtliche Zahlen α, β, γ etc. teilbare Zahl und P eine Primfunktion vom Grade π. Dann hat nach dem Vorhergehenden jede der Kongruenzen

$$A(y) \equiv 0 \pmod{P}, \qquad B(y) \equiv 0 \pmod{P}, \quad \text{etc.}$$

ebensoviel inkongruente Wurzeln, als ihr Grad beträgt, und zwar ist der Grad die Zahl, zu welcher die Wurzeln passen. Daraus folgt, daß man stets eine identische Kongruenz von der Form

$$M(y) \equiv E\{\Pi(y - A')\}^a\{\Pi(y - B')\}^b \cdots \pmod{P}$$

aufstellen kann, in welcher

$$\Pi(y - A') = (y - A')(y - A'^p) \cdots (y - A'^{p^{\alpha-1}})$$

und A' eine Funktion ist, welche zum Divisor α von π paßt.

22.

Man kann endlich auch das Produkt aller primären Primfunktionen eines bestimmten Grades m isoliert darstellen, mit Hilfe eines Satzes, welcher dem im Art. 18 ohne Beweis angeführten analog ist und durch einen logarithmischen Übergang leicht aus diesem abgeleitet werden kann. Dazu führt folgender Gedankengang. Sind a, b zwei ganze positive Zahlen, und ist $c < b$ der bei der Division von a durch b bleibende (nicht negative) Rest, so ist $x^c - 1$ der Rest, welcher bei der algebraischen Division von $x^a - 1$ durch $x^b - 1$ bleibt; und dies bleibt auch noch richtig, wenn man für x eine beliebige positive ganze Zahl p einsetzt. Ist daher h der größte gemeinschaftliche Teiler von a, b, so ist algebraisch $x^h - 1$ der größte gemeinschaftliche Teiler von $x^a - 1$, $x^b - 1$; und ebenso ist im gewöhnlichen Sinne $p^h - 1$ der größte gemeinschaftliche Teiler von $p^a - 1$, $p^b - 1$. Daraus folgt durch abermalige Anwendung desselben Satzes, daß algebraisch $x^{p^h - 1} - 1$ der größte gemeinschaftliche Teiler von $x^{p^a - 1} - 1$, $x^{p^b - 1} - 1$, und also auch $x^{p^h} - x$ der größte gemeinschaftliche Teiler von $x^{p^a} - x$, $x^{p^b} - x$ ist.

Sei nun m irgend eine positive ganze Zahl, welche durch keine anderen Primzahlen als a, b, c, $\cdots$ teilbar ist, so folgt aus den vorhergehenden Prinzipien, daß

$$(x^{p^m} - x) : \Pi(x^{p^{\frac{m}{a}}} - x) \times \Pi(x^{p^{\frac{m}{ab}}} - x) : \Pi(x^{p^{\frac{m}{abc}}} - x) \times \cdots$$

eine ganze Funktion ist; hierin bezieht sich das Produkt-Zeichen Π der Reihe nach auf die verschiedenen Kombinationen zu 1, 2, 3 usw.; und die mit einander abwechselnden Divisions- und Multiplikationszeichen beziehen sich jedesmal nur auf das zunächst folgende Produkt.

Nehmen wir nun hierin p als Primzahl an, so ergibt sich aus den vorhergehenden Artikeln, daß die nach dem soeben bezeichneten Gesetz gebildete ganze Funktion in bezug auf den Modul p kongruent ist dem Produkte aus allen inkongruenten primären Primfunktionen vom Grade m. Der Grad dieser Funktion ist, übereinstimmend mit Art. 18, gleich

$$p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots.$$

Die gemeinschaftliche Quelle des im Art. 18 angeführten und des analogen soeben benutzten Satzes ist folgende. Sei m irgend

eine ganze Zahl, ferner a, b, c, ..., k sämtliche voneinander verschiedene in m aufgehende Primzahlen; man bilde zwei getrennte Komplexe D, D' von Divisoren der Zahl m nach folgendem Prinzip. In den Komplex D nehme man zunächst alle Divisoren der Zahl m auf; in den Komplex D' alle Divisoren von $\frac{m}{a}$, alle Divisoren von $\frac{m}{b}$ usw.; dann wieder in den Komplex D alle Divisoren von $\frac{m}{ab}$, von $\frac{m}{ac}$, von $\frac{m}{bc}$ usw.; dann wieder in den Komplex D' alle Divisoren von $\frac{m}{abc}$ usw., bis man endlich auch alle Divisoren von $\frac{m}{abc\ldots k}$ entweder in den Komplex D oder in den Komplex D' aufgenommen hat, je nachdem die Anzahl der Primzahlen a, b, c, ..., k eine gerade oder ungerade ist. Dann ist leicht zu zeigen, daß jeder Divisor der Zahl m ebenso oft in dem einen wie in dem anderen Komplex vorkommt, mit Ausnahme des Divisors m selbst, der lediglich und nur ein einziges Mal in dem Komplex D vorkommt. Es bedarf nur eines Blickes, um hieraus die Umkehrungen der Gleichungen

$$\Sigma f(\delta) = F(m) \quad \text{oder} \quad \Pi f(\delta) = F(m)$$

abzuleiten, in welchen das Summen- oder Produkt-Zeichen Σ oder Π sich auf sämtliche Divisoren δ einer beliebigen Zahl m bezieht; diese Auflösungen sind in den Formeln

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \cdots$$

oder

$$f(m) = F(m) : \Pi F\left(\frac{m}{a}\right) \times \Pi F\left(\frac{m}{ab}\right) : \cdots$$

enthalten.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Die Resultate dieser Abhandlung befinden sich schon zum größten Teil in den in der Einleitung erwähnten Abhandlungen von Galois, Serret und Schönemann; bei Galois und Serret werden aber die Resultate unter Anwendung der Galoisschen Imaginären, bei Schönemann durch eine algebraische Betrachtungsweise unter Anwendung des Fundamentalsatzes der Algebra abgeleitet. Dedekind

reduziert hier die Theorie auf ihre einfachste, rein zahlentheoretische Form, wodurch auch die ganze Theorie der Galoisschen Imaginären überflüssig gemacht wird.

Der Restbereich für den Doppelmodul (modd. p, $P(x)$) [$P(x)$ Primfunktion (mod. p) vom Grade π] bilden offenbar einen endlichen Körper (Galoissches Feld) von der Charakteristik p mit p^π Elementen. Nach einem bekannten Satz von E. H. Moore (Papers read at the international mathematical congress, Chicago 1893 (1896), S. 208—226) ist jeder endliche Körper mit einem solchen Restbereich (modd. p, $P(x)$) isomorph und die vorstehende Dedekindsche Abhandlung gibt daher sogleich die arithmetische und zum Teil die algebraische Theorie der endlichen Körper. Für die algebraischen Eigenschaften der endlichen Körper und ihre Erweiterungen muß auf die Arbeit von E. Steinitz, Algebraische Theorie der Körper, Journ. f. Math., Bd. 137 (1910) hingewiesen werden.

Zuletzt sei noch erwähnt, daß diese Abhandlung eine wichtige Grundlage für die spätere Arbeit: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, bildet.

Ore.

VI.

Beweis für die Irreduktibilität der Kreisteilungs-Gleichungen.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 27—30 (1857)].

Nachdem Gauß[*)] zuerst die Irreduktibilität der Gleichung $\frac{x^p - 1}{x - 1} = 0$ für den Fall bewiesen hatte, daß p eine Primzahl ist, lag es nahe, einen ähnlichen Satz zu vermuten, welcher sich auf die Teilung des Kreisumfangs in eine beliebige Anzahl m gleicher Teile bezieht. Dieser Satz wird so lauten:

„Die Gleichung vom Grade $\varphi(m)$, welche sämtliche $\varphi(m)$ primitive Wurzeln der Gleichung $x^m = 1$ zu Wurzeln hat, ist irreduktibel."

Dem Beweis von Gauß folgte zunächst eine Reihe anderer von Kronecker, Schönemann, Eisenstein, die auf wesentlich verschiedenen Prinzipien beruhen, sich aber sämtlich auf denselben einfachsten Fall beziehen, in welchem m eine Primzahl ist. Doch sieht man leicht, daß diese Prinzipien auch noch auf den Fall anwendbar sind, in welchem m nur durch eine einzige Primzahl teilbar, also eine Potenz dieser Primzahl ist, und namentlich wurden die Beweise von Kronecker und Eisenstein in diesem Sinne von Serret verallgemeinert. Allein diese Prinzipien reichen nicht mehr aus, sobald die Zahl m durch mehrere Primzahlen teilbar ist, weil dann die in Rede stehende Gleichung in verschiedener Hinsicht einen wesentlich anderen Charakter annimmt. Auf diesen Punkt hat zuerst Kronecker[**)] in einer Abhandlung aufmerksam gemacht, welche zugleich den ersten Beweis des obigen, und zwar noch verallgemeinerten Theorems enthält. Obgleich nun dieser Satz für die algebraische Auflösung der Gleichung $x^m = 1$ nicht gerade erforderlich ist, da diese bekanntlich immer auf den Fall zurückgeführt werden kann, in welchem m die Potenz einer einzigen Primzahl ist, so verdient doch vielleicht

[*) Ein vollständiges Literaturverzeichnis über die verschiedenen Beweise für die Irreduzibilität der Kreisteilungsgleichung findet man in: Dickson, Mitchell, Vandiver, Wahlin, Algebraic numbers § 13. Bulletin of the National Research Council, Vol. 5, part 3, no. 28 (1923)].

[**) L. Kronecker, Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. Journ. de Math. Bd. 19, S. 177—192 (1854)].

ein neuer Beweis desselben, der sich durch seine Einfachheit auszeichnet, die Aufmerksamkeit derjenigen Mathematiker, welche sich mit diesem Teile der Algebra beschäftigen.

1.

Der neue Beweis stützt sich auf elementare Sätze über die Kongruenzen höherer Grade, und ich werde mich in dieser Beziehung auf den vorstehenden Aufsatz über die Theorie derselben berufen; außerdem benutze ich noch den folgenden zuerst von Schönemann[*)] bewiesenen Satz: Ist

$$f(x) = (x-\alpha)(x-\beta)\cdots(x-\lambda)$$

eine ganze rationale Funktion mit reellen ganzzahligen Koeffizienten, p eine absolute Primzahl und

$$f_1(x) = (x-\alpha^p)(x-\beta^p)\cdots(x-\lambda^p),$$

so sind die Koeffizienten dieser letzteren Funktion ebenfalls ganze reelle Zahlen, und zwar den entsprechenden Koeffizienten von $f(x)$ kongruent nach dem Modulus p, in Zeichen

$$f_1(x) \equiv f(x) \pmod{p}.$$

Für den direkten Beweis dieses Satzes, welcher eigentlich nur eine sehr spezielle algebraische Anwendung der genannten Theorie der höheren Kongruenzen ist, mag hier folgende Bemerkung genügen. Sieht man $\alpha, \beta, \ldots, \lambda$ als ganz unbestimmte Größen an und bezeichnet mit A und A_1 irgend zwei einander entsprechende Koeffizienten der beiden Funktionen $f(x)$ und $f_1(x)$, so leuchtet ein, daß man $A^p = A_1 + pA_2$ setzen kann, worin A_1 und A_2 ganze, ganzzahlige und zugleich symmetrische Funktionen von $\alpha, \beta, \ldots, \lambda$ und folglich auch (nach dem Fundamentalsatze über die Transformation symmetrischer Funktionen) ganze und ganzzahlige Funktionen der Koeffizienten A von $f(x)$ sind. Sind daher diese Koeffizienten ganze reelle Zahlen, so erhält man $A^p \equiv A_1 \pmod{p}$, und nach dem Fermatschen Satze also auch $A \equiv A_1 \pmod{p}$, was zu beweisen war.

2.

Es sei nun α irgend eine primitive Wurzel der Gleichung $x^m = 1$ und $f(x)$ der durch $x-\alpha$ teilbare irreduktibele Faktor von $x^m - 1$, dessen rationale Koeffizienten sämtlich ganze Zahlen sein müssen,

[*) Th. Schönemann, Grundzüge einer allgemeinen Theorie der höheren Kongruenzen, deren Modul eine reelle Primzahl ist; § 13. Journ. f. Math. Bd. 31, S. 269—325 (1846)].

wenn der der höchsten Potenz von x gleich Eins angenommen wird (Disqu. Arithm. Art. 42). Der zu beweisende Satz ist dann identisch mit dem folgenden: „Die Gleichung $f(x) = 0$ hat zu Wurzeln sämtliche $\varphi(m)$ primitive $m$te Wurzeln der Einheit, und keine anderen.“ Der Beweis des letzteren Teiles dieses Satzes hat keine Schwierigkeit, soll aber doch der Vollständigkeit halber hier nicht übergangen werden. Ist α^r irgend eine Wurzel der Gleichung $f(x) = 0$ — und in dieser Form sind ja alle ihre Wurzeln enthalten —, so folgt in bekannter Weise aus der Irreduktibilität von $f(x)$, daß jedes Glied der Reihe α^r, α^{r^2}, α^{r^3}, $\cdots$ eine Wurzel der Gleichung ist, und daß in dieser Reihe früher oder später einmal ein Glied α^{r^n} kommen muß, welches $= \alpha$ ist; daraus folgt aber $r^n \equiv 1 \pmod{m}$, und es ist daher r relative Primzahl gegen m, und folglich α^r ebenfalls eine primitive $m$te Wurzel der Einheit.

Ungleich schwieriger ist der Nachweis des ersten Teiles, daß nämlich umgekehrt jede primitive $m$te Wurzel der Einheit (d. h. jedes α^r, wenn r relative Primzahl gegen m ist) der Gleichung $f(x) = 0$ genügt; doch kann man das Problem sogleich auf den einfachsten Fall reduzieren, in welchem r eine absolute Primzahl ist, die natürlich nicht in m aufgehen darf. Ist nämlich bewiesen, daß α^r, α^s der Gleichung $f(x) = 0$ genügen, so muß auch $\alpha^{r \cdot s}$ ihr genügen; denn da der Annahme nach α der rationalen Gleichung $f(x^r) = 0$ genügt, so muß ihr auch jede andere Wurzel α^s der irreduktibeln Gleichung $f(x) = 0$ genügen. Offenbar braucht also nur noch gezeigt zu werden, daß jedes α^p der Gleichung $f(x) = 0$ genügt, wenn p eine absolute Primzahl ist, welche nicht in m aufgeht.

3.

Um dies zu beweisen, bemerken wir, daß die Wurzeln der irreduktibeln Gleichung $f_1(x) = 0$, welcher α^p genügt, mit den $p$ten Potenzen der Wurzeln der Gleichung $f(x) = 0$ übereinstimmen müssen; denn da α^p ebensowohl eine rationale Funktion von α, wie umgekehrt α von α^p ist (nämlich $= (\alpha^p)^{p'}$, wenn $pp' \equiv 1 \pmod{m}$), so müssen die Grade der beiden Funktionen $f(x)$ und $f_1(x)$ einander gleich sein. Setzt man daher

$$f(x) = (x - \alpha)(x - \beta) \cdots (x - \lambda),$$

so ist

$$f_1(x) = (x - \alpha^p)(x - \beta^p) \cdots (x - \lambda^p)$$

und folglich nach dem oben bewiesenen Satze von Schönemann

$$f_1(x) \equiv f(x) \pmod{p}.$$

Und aus dieser Kongruenz zwischen den beiden Funktionen $f(x)$ und $f_1(x)$ folgt auch ihre Identität. Denn nehmen wir an, die beiden irreduktibeln Funktionen $f(x)$ und $f_1(x)$ sind nicht identisch, so können sie auch keinen gemeinschaftlichen Faktor haben, und folglich ist $x^m - 1$ durch ihr Produkt teilbar, da $x^m - 1$ sowohl durch $f(x)$ als auch durch $f_1(x)$ teilbar ist. Es wäre daher $x^m - 1$ einem Produkt von Faktoren gleich, unter denen mindestens zwei einander nach dem Modulus p kongruent wären. Dann müßte (zufolge Art. 6 des vorstehenden Aufsatzes über die höheren Kongruenzen) die Funktion $x^m - 1$ mit ihrer ersten Derivierten mx^{m-1} nach dem Modulus p gemeinschaftliche Divisoren haben; da aber m nicht durch p teilbar, und folglich mx^{m-1} auch nicht $\equiv 0 \pmod{p}$ ist, so hat mx^{m-1} nach dem Modulus p nur solche primäre Primfaktoren, welche $\equiv x$ sind; und offenbar hat $x^m - 1$ keinen solchen Primfaktor nach dem Modulus p, da sonst für $x \equiv 0$ auch $x^m - 1 \equiv 0$ werden müßte, was ja nicht der Fall ist.

Mithin sind die beiden Funktionen $f(x)$ und $f_1(x)$ identisch; jedes α^p und folglich auch jedes α^r genügt also einer und derselben irreduktibeln Gleichung $f(x) = 0$, wenn r relative Primzahl gegen m ist. W. Z. B. W.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Der vorliegende Dedekindsche Beweis der Irreduzibilität der allgemeinen Kreisteilungsgleichung ist in bezug auf Einfachheit dem S. 68 zitierten Kroneckerschen Beweise überlegen, obwohl die Verallgemeinerung auf die Irreduzibilität in Körpern, deren Diskriminante zu m relativ prim ist, nicht so einfach wird. Der Dedekindsche Beweis ist in H. Weber, Algebra, 2. Aufl. (1898), Bd. 1, S. 596—600 reproduziert.

F. Mertens (Sitzungsber. d. Akad. d. Wiss. in Wien 1905, IIa, S. 1293—96) hat eine Vereinfachung des Dedekindschen Beweises vorgeschlagen, indem er direkt beweist, daß wenn r zu m relativ prim ist, dann $f(x^r)$ algebraisch durch $f(x)$ teilbar sein muß (Bezeichnung von § 2). Das Dedekindsche Prinzip ist auch im Beweise von H. Späth (Math. Zeitschr. Bd. 26, S. 442—444 (1927)) angewandt. Aber die Dedekindsche Vereinfachung, daß r als Primzahl angenommen werden darf, ist von diesen Autoren nicht übernommen.

Ore.

VII.

Ableitung der allgemeinen Form der Kugelfunktionen.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1859, S. 346–362.]

1.

Dieses Problem ist auf verschiedene Arten von Laplace, Jacobi, Dirichlet behandelt; im folgenden soll ein mehr elementarer Weg eingeschlagen werden. Wir gehen von nachstehender Definition aus: „Unter einer Kugelfunktion n^{ter} Ordnung wird jede ganze rationale Funktion Y der drei Kugelkoordinaten

$$\cos\Theta,\quad \sin\Theta\cos\varphi,\quad \sin\Theta\sin\varphi$$

verstanden, welche der partiellen Differentialgleichung

$$(I)\qquad n(n+1)\sin\Theta\cdot Y+\frac{d}{d\Theta}\left(\sin\Theta\frac{dY}{d\Theta}\right)+\frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2}=0$$

Genüge leistet.“ Bekanntlich ist dann sowohl $v=\varrho^n Y$, als auch $v=\varrho^{-(n+1)}Y$ eine Lösung der Differentialgleichung

$$(II)\qquad \sin\Theta\cdot\frac{d}{d\varrho}\left(\varrho^2\frac{dv}{d\varrho}\right)+\frac{d}{d\Theta}\left(\sin\Theta\frac{dv}{d\Theta}\right)+\frac{1}{\sin\Theta}\frac{d^2v}{d\varphi^2}=0$$

oder, als Funktion der drei rechtwinkligen Parallelkoordinaten $\xi=\varrho\cos\Theta$, $\eta=\varrho\sin\Theta\cos\varphi$, $\zeta=\varrho\sin\Theta\sin\varphi$ angesehen, eine Lösung der Gleichung

$$(III)\qquad \frac{d^2v}{d\xi^2}+\frac{d^2v}{d\eta^2}+\frac{d^2v}{d\zeta^2}=0.$$

Wir wollen indessen lediglich die Gleichung (I) unserer Untersuchung zugrunde legen.

2.

Da Y eine ganze rationale Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$, also eine Summe von Gliedern der Form

$$Const\cdot\cos\Theta^{\alpha}\sin\Theta^{\beta+\gamma}\cos\varphi^{\beta}\sin\varphi^{\gamma}$$

sein soll, worin α, β, γ ganze positive Zahlen oder Null sind, eine solche Funktion aber infolge der Identität

$$\cos\Theta^2 + (\sin\Theta\cos\varphi)^2 + (\sin\Theta\sin\varphi)^2 = 1$$

auf unendlich viele verschiedene Arten umgeformt werden kann, ohne diesen Charakter zu verlieren, so ist es zweckmäßig, zunächst eine Normalform festzusetzen, in welche jede solche Funktion stets, und auch nur auf eine einzige Weise, gebracht werden kann, und welche umgekehrt auch keine anderen als solche Funktionen enthält.

Zu einer solchen Darstellungsform gelangen wir leicht durch die folgende Bemerkung. Aus den Formeln für die Umwandlung der Produkte $2\sin a\sin b$, $2\cos a\cos b$, $2\sin a\cos b$ in eine Summe zweier Kosinus oder Sinus ergibt sich bekanntlich, daß man stets, je nachdem γ gerade oder ungerade ist,

$$\cos\varphi^\beta\sin\varphi^\gamma = a\cos(\beta+\gamma)\varphi + a_1\cos(\beta+\gamma-2)\varphi + a_2\cos(\beta+\gamma-4)\varphi + \cdots$$

oder

$$\cos\varphi^\beta\sin\varphi^\gamma = b\sin(\beta+\gamma)\varphi + b_1\sin(\beta+\gamma-2)\varphi + b_2\sin(\beta+\gamma-4)\varphi + \cdots$$

setzen kann, worin $a, a_1, a_2 \ldots$ und $b, b_1, b_2 \ldots$ bestimmte Zahlkoeffizienten bedeuten. Da nun ferner

$$\sin\Theta^{\beta+\gamma} = (1-\cos\Theta^2)\sin\Theta^{\beta+\gamma-2} = (1-\cos\Theta^2)^2\sin\Theta^{\beta+\gamma-4} = \cdots$$

ist, so leuchtet ein, daß man jedes einzelne Glied einer rationalen ganzen Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ und folglich auch die ganze Funktion selbst in die Form

$$(1) \qquad \sum_{s=0}^{s=k}(y_s\cos s\varphi + z_s\sin s\varphi)\sin\Theta^s$$

bringen kann, wo y_s und z_s rationale Funktionen von $\cos\Theta$ sind und k den größten Wert von $\beta+\gamma$ bedeutet.

Daß eine rationale ganze Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ nur auf eine einzige Weise in diese Form gebracht werden kann, d. h. daß zwei solche Summen von der vorstehenden Form (1) nur dann identisch sein können, wenn die einzelnen Glieder, also auch die Funktionen y_s, z_s der einen Summe mit den entsprechenden der anderen Summe identisch sind, ist bekannt und läßt sich am kürzesten durch Multiplikation mit $\cos s\varphi\cdot d\varphi$, oder mit $\sin s\varphi\cdot d\varphi$ und Integration zwischen den Grenzen 0 und 2π beweisen.

Daß endlich umgekehrt jede solche Summe von der Form (1) auch eine ganze rationale Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ ist, folgt unmittelbar aus dem Moivreschen Satze

$$\sin\Theta^s\cos s\varphi + i\sin\Theta^s\sin s\varphi = (\sin\Theta\cos\varphi + i\sin\Theta\sin\varphi)^s,$$

worin $i = \sqrt{-1}$ ist.

Also ist die Form (1) eine solche oben verlangte Normalform.

3.

Wir haben jetzt die allgemeinste Form der rationalen ganzen Funktionen y_s, z_s von $\cos\Theta$ zu suchen, für welche der Ausdruck (1) eine Kugelfunktion n^{ter} Ordnung wird, d. h. der Differentialgleichung (I) genügt. Bezeichnen wir zur Abkürzung $\cos\Theta$, soweit diese Größe in den Funktionen y_s, z_s vorkommt, mit x, so daß also $dx = -\sin\Theta\cdot d\Theta$ ist, und unterwerfen wir den Ausdruck (1) der Differentialgleichung (I), so erhalten wir (da nach dem Vorhergehenden der Koeffizient von $\cos s\varphi$, sowie der von $\sin s\varphi$ in der entstehenden Gleichung für sich $= 0$ sein muß) das Resultat, daß die beiden rationalen ganzen Funktionen y_s, z_s von $x = \cos\Theta$ Lösungen der linearen Differentialgleichung 2^{ter} Ordnung

$$[s] \qquad [n(n+1) - s(s+1)]u - 2(s+1)x\frac{du}{dx} + (1-x^2)\frac{d^2u}{dx^2} = 0$$

sein müssen. Und umgekehrt leuchtet ein, daß dann der Ausdruck (1) eine Kugelfunktion n^{ter} Ordnung sein wird.

Diese Differentialgleichung $[s]$ wollen wir nun untersuchen, dabei aber auch die Fälle betrachten, in welchen s eine negative ganze Zahl ist, während wir n stets als ganze positive Zahl oder Null voraussetzen. Durch Differentiation der Gleichung $[s]$ erhalten wir

$$[n(n+1) - (s+1)(s+2)]\frac{du}{dx} - 2(s+2)x\frac{d^2u}{dx^2} + (1-x^2)\frac{d^3u}{dx^3} = 0,$$

woraus unmittelbar der Satz folgt: Genügt u der Gleichung $[s]$, so genügt $\frac{du}{dx}$ der Gleichung $[s+1]$, und folglich $\frac{d^ru}{dx^r}$ der Gleichung $[s+r]$, wenn r eine beliebige ganze positive Zahl bedeutet.

Nun finden wir aber für $s = -(n+1)$, daß das allgemeine Integral der Gleichung

$$[-(n+1)] \qquad 2nx\frac{du}{dx} + (1-x^2)\frac{d^2u}{dx^2} = 0$$

die Funktion

$$c\int(x^2-1)^n\,dx + c_1$$

ist, folglich ist nach dem eben bewiesenen Satz

$$c\frac{d^{n+s}(x^2-1)^n}{dx^{n+s}} = cD^{n+s}(x^2-1)^n$$

eine Lösung der Gleichung [s], und zwar ist diese Lösung eine ganze rationale Funktion von x. Sie gilt für alle ganzen Zahlenwerte von s zwischen $-n$ und $+n$.

Jetzt soll noch bewiesen werden, daß für alle ganzen Zahlwerte von s zwischen 0 und $+n$ jede rationale ganze Auflösung der Gleichung [s] in der eben gefundenen Form enthalten ist. Denn, wenn y und z irgend zwei von Null verschiedene Lösungen der Gleichung [s] sind, also

$$[n(n+1)-s(s+1)]\,y - 2(s+1)\,x\frac{dy}{dx} + (1-x^2)\frac{d^2y}{dx^2} = 0\,.$$

$$[n(n+1)-s(s+1)]\,z - 2(s+1)\,x\frac{dz}{dx} + (1-x^2)\frac{d^2z}{dx^2} = 0$$

ist, so folgt hieraus unmittelbar

$$-2(s+1)\,x\left\{z\frac{dy}{dx} - y\frac{dz}{dx}\right\} + (1-x^2)\left\{z\frac{d^2y}{dx^2} - y\frac{d^2z}{dx^2}\right\} = 0,$$

und da

$$z\frac{d^2y}{dx^2} - y\frac{d^2z}{dx^2} = \frac{d}{dx}\left\{z\frac{dy}{dx} - y\frac{dz}{dx}\right\}$$

ist, so erhält man durch Integration

$$z\frac{dy}{dx} - y\frac{dz}{dx} = \frac{Const}{(x^2-1)^{s+1}}.$$

Sind nun y und z ganze rationale Funktionen von x, und ist s eine der Zahlen 0, 1, 2, ... n, so kann diese Gleichung nur bestehen, wenn $Const = 0$ ist; daraus folgt

$$z\frac{dy}{dx} = y\frac{dz}{dx}, \quad z = Const.\,y,$$

was zu beweisen war.

Da auf diese Weise die allgemeinste Form der Funktionen y_s, z_s für ein positives $s \gtreqless n$ gefunden ist, so fragt sich nur noch, ob auch für $s > n$ ganze rationale Lösungen der Gleichung [s] existieren. Nimmt man an, daß r der Grad einer solchen Lösung sei, so erhält man unmittelbar durch Einsetzen in die Differentialgleichung [s] und Vergleichung der Koeffizienten von x^r die Gleichung

$$n(n+1) - s(s+1) - 2(s+1)r - r(r-1) = 0$$

oder

$$n(n+1) - (r+s)(r+s+1) = 0,$$

woraus

$$r + s = n \quad \text{oder} \quad = -(n+1)$$

folgt. Ist daher $s > n$, so würde in beiden Fällen r negativ ausfallen; also existiert keine solche Lösung.

Auf diese Weise haben wir als die allgemeinste Form einer Kugelfunktion n^{ter} Ordnung

$$Y = \sum_{s=0}^{s=n} (\alpha_s \cos s\varphi + \beta_s \sin s\varphi) D^{n+s}(x^2-1)^n \cdot \sin\Theta^s$$

gefunden, in welcher α_s, β_s ganz willkürliche Konstanten bedeuten, deren Anzahl $= 2n+1$ ist, und wo $x = \cos\Theta$ ist.

4.

Obgleich im vorhergehenden die ursprüngliche Aufgabe ihre vollständige Lösung erhalten hat, so wird es doch nicht unangemessen sein, die schönen Sätze von Jacobi u. a. aus derselben Quelle, aus der Differentialgleichung $[s]$ abzuleiten.

Ist s eine ganze Zahl zwischen 0 und $+n$, so folgt aus dem vorigen Artikel, daß

$$D^{n-s}(x^2-1)^n$$

eine Lösung der Differentialgleichung $[-s]$ ist; diese ganze Funktion ist offenbar teilbar durch $(x^2-1)^s$; setzen wir daher

$$D^{n-s}(x^2-1)^n = (x^2-1)^s w,$$

und suchen wir die ganze Funktion w zu bestimmen.

Setzen wir, ganz abgesehen von der dem w beigelegten speziellen Bedeutung, den Ausdruck $(x^2-1)^s w$ in die Differentialgleichung $[-s]$ ein, so ergibt sich, daß w der Gleichung $[s]$ genügen muß, woraus der allgemeine Satz folgt: Wenn w der Differentialgleichung $[s]$ genügt, so genügt $(x^2-1)^s w$ der Differentialgleichung $[-s]$, und umgekehrt.

Dies auf unseren Fall angewendet (in welchem $0 \gtreqless s \gtreqless +n$) gibt das Resultat, daß die ganze Funktion

$$w = Const \cdot D^{n+s}(x^2-1)^n$$

sein muß.

Setzt man dies in die vorige Gleichung ein, so erhält man durch Vergleichung der Koeffizienten von x^{n+s} auf beiden Seiten, den Satz von Jacobi:

$$D^{n-s}(x^2-1)^n = \frac{\Pi(n-s)}{\Pi(n+s)}(x^2-1)^s D^{n+s}(x^2-1)^n,$$

der zwar nur für $0 \leqq s \leqq n$ bewiesen ist, dessen Richtigkeit aber unmittelbar auf das ganze Intervall $-n \lessgtr s \lessgtr +n$ übertragen werden kann.

Durch wiederholte teilweise Integration findet man leicht, daß

$$\int_{-1}^{+1} D^m(x^2-1)^m D^n(x^2-1)^n dx = (-1)^s \int_{-1}^{+1} D^{m-s}(x^2-1)^m D^{n+s}(x^2-1)^n dx$$

$$= (-1)^m \int_{-1}^{+1} (x^2-1)^m D^{n+m}(x^2-1)^n dx$$

ist. Hieraus folgt unmittelbar

$$\int_{-1}^{+1} D^m(x^2-1)^m D^n(x^2-1)^n dx = 0,$$

wenn $m > n$, und folglich auch, da die linke Seite symmetrisch in bezug auf m und n ist, wenn $m < n$. Ist aber $m = n$, so folgt

$$\int_{-1}^{+1} [D^n(x^2-1)^n]^2 dx = \Pi(2n) \cdot \int_{-1}^{+1} (1-x^2)^n dx;$$

da nun

$$\int (1-x^2)^n dx = \frac{x(1-x^2)^n}{2n+1} + \frac{2n}{2n+1} \int (1-x^2)^{n-1} dx$$

ist, so ist

$$\int_{-1}^{+1} (1-x^2)^n dx = \frac{2n}{2n+1} \int_{-1}^{+1} (1-x^2)^{n-1} dx = \frac{2n(2n-2)\cdots 4 \cdot 2}{(2n+1)(2n-1)\cdots 5 \cdot 3} \cdot 2,$$

folglich

$$\int_{-1}^{+1} [D^n(x^2-1)^n]^2 dx = \frac{2}{2n+1} \cdot [2^n \Pi(n)]^2.$$

Wir bedürfen endlich noch des Wertes von $D^{n+s}(x^2-1)^n$ für $x = 1$, den wir mit h_s bezeichnen wollen. Da $D^{n+s}(x^2-1)^n$ der Differentialgleichung $[s]$ genügt, so ergibt sich

$$[n(n+1) - s(s+1)]h_s - 2(s+1)h_{s+1} = 0,$$

also

$$h_s = \frac{2(s+1)}{(n-s)(n+s+1)} h_{s+1} = \frac{\Pi(n+s)}{\Pi(n-s)} \cdot \frac{2^n \Pi(n)}{2^s \Pi(s)},$$

da $h_n = \Pi(2n)$ ist.

5.

Nehmen wir auf einer mit einem Radius $= 1$ beschriebenen Kugelfläche einen bestimmten Punkt p als Pol eines Polarkoordinatensystems, indem wir mit Θ die Polardistanz $p\mu$ irgend eines Punktes μ der Kugelfläche, mit φ den Winkel bezeichnen, den der Meridian $p\mu$ mit einem festen Meridian bildet, so kann jede Funktion $f(\Theta, \varphi)$ von Θ, φ innerhalb der Grenzen $0 < \Theta < \pi$, $0 < \varphi < 2\pi$, als Funktion des Ortes eines Punktes μ auf dieser Kugelfläche angesehen werden. Es sei nun σ ein beliebig begrenzter Teil dieser Kugelfläche, ds ein unendlich kleines Element seiner Begrenzung, N die in ds nach innen errichtete sphärische Normale; ferner mögen Y, Z zwei Funktionen von Θ, φ sein, welche nebst ihren ersten partiellen Derivierten innerhalb des Gebietes σ endlich und stetig sind. Dann findet man

$$\iint \left\{ \frac{d}{d\Theta}\left(Z \sin\Theta \frac{dY}{d\Theta}\right) + \frac{d}{d\varphi}\left(Z \frac{1}{\sin\Theta}\frac{dY}{d\varphi}\right)\right\} d\Theta\, d\varphi = -\int Z \frac{dY}{dN}\, ds,$$

worin das Doppelintegral linker Hand über alle Werte Θ, φ auszudehnen ist, denen Punkte innerhalb σ entsprechen, während rechts die Integration sich über die ganze Begrenzung s von σ erstreckt und $\frac{dY}{dN}$ die in der Richtung der nach innen errichteten Normale N genommene Derivierte von Y bedeutet. Um sich von der Richtigkeit dieses Satzes zu überzeugen, braucht man nur an jedem der beiden Teile links eine Integration auszuführen.

Andererseits ist aber

$$\frac{d}{d\Theta}\left(Z \sin\Theta \frac{dY}{d\Theta}\right) + \frac{d}{d\varphi}\left(Z \frac{1}{\sin\Theta}\frac{dY}{d\varphi}\right)$$
$$= Z\left\{\frac{d}{d\Theta}\left(\sin\Theta \frac{dY}{d\Theta}\right) + \frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2}\right\} + \sin\Theta \frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta}\frac{dZ}{d\varphi}\frac{dY}{d\varphi};$$

ist daher Y eine Kugelfunktion n^{ter} Ordnung, also

$$\frac{d}{d\Theta}\left(\sin\Theta \frac{dY}{d\Theta}\right) + \frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2} = -n(n+1)\sin\Theta \cdot Y,$$

so erhalten wir folgenden Satz:

(IV) $$n(n+1)\int ZY\, d\sigma - \int \left\{\frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta^2}\frac{dZ}{d\varphi}\frac{dY}{d\varphi}\right\} d\sigma = \int Z \frac{dY}{dN}\, ds,$$

worin $d\sigma = \sin\Theta\, d\Theta\, d\varphi$ ein unendlich kleines Element von σ bedeutet, und die Integrationen links über σ, rechts über die Be-

grenzung s von σ auszudehnen sind. Für $Z = 1$ erhalten wir das Resultat

$$(V) \qquad n(n+1)\int Y\, d\sigma = \int \frac{dY}{dN}\, ds,$$

und diese Gleichung ist nur als eine Transformation der Fundamentalgleichung (I) anzusehen, welche sich umgekehrt wieder aus (V) ableiten läßt, sobald man für σ das von zwei unendlich nahen Parallelkreisen (Θ und $\Theta + d\Theta$) und zwei unendlich nahen Meridianen (φ und $\varphi + d\varphi$) begrenzte Flächenelement $d\sigma = \sin\Theta\, d\Theta\, d\varphi$ wählt. Diese Gleichung (V) spricht aber eine, von dem zufällig gewählten Polarkoordinatensystem (Θ, φ) ganz unabhängige, geometrische Eigenschaft der Ortsfunktion Y aus; nimmt man daher ein beliebiges anderes Polarkoordinatensystem, d. h. einen neuen Pol p' und einen neuen Anfangsmeridian, und bezeichnet mit ω die neue Polardistanz $p'\mu$, mit ψ den Winkel, den der Meridian $p'\mu$ mit dem neuen Anfangsmeridian bildet, so muß Y, als Funktion der neuen Koordinaten ω, ψ, der partiellen Differentialgleichung

$$(VI) \qquad n(n+1)\sin\omega\, Y + \frac{d}{d\omega}\left(\sin\omega\, \frac{dY}{d\omega}\right) + \frac{1}{\sin\omega}\, \frac{d^2Y}{d\psi^2} = 0$$

Genüge leisten. Ferner ist aus der Theorie der Transformation orthogonaler Koordinaten bekannt, daß jede der drei Größen

$$\cos\Theta, \quad \sin\Theta\cos\varphi, \quad \sin\Theta\sin\varphi$$

eine homogene lineare Funktion der drei Größen

$$\cos\omega, \quad \sin\omega\cos\psi, \quad \sin\omega\sin\psi$$

ist (und umgekehrt). Also ist Y auch eine ganze rationale Funktion dieser drei letzten Größen. Wir sehen also, daß die ursprünglich aufgestellte Definition einer Kugelfunktion ganz unabhängig ist von dem zugrunde gelegten Koordinatensystem. Bezeichnen wir daher zur Abkürzung $\cos\omega$ mit λ, so findet stets eine Identität von folgender Form statt:

$$Y = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi)\sin^s\Theta \cdot D^{n+s}(x^2-1)^n$$

$$= \sum_0^n (a_s \cos s\psi + b_s \sin s\psi)\sin^s\omega \cdot D^{n+s}(\lambda^2-1)^n.$$

6.

Wir benutzen die Resultate des vorigen Artikels, um folgende Aufgabe zu lösen: Die allgemeinste Form einer Kugelfunktion n^{ter} Ordnung

$$P = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi) \sin\Theta^s \cdot D^{n+s}(x^2-1)^n$$

zu finden, welche auf jedem einzelnen eines Systems von Parallelkreisen von gegebener Lage einen konstanten Wert hat.

Die Lage des Systems von Parallelkreisen ist durch die Lage des Pols p' derselben gegeben; bezeichnen wir die Koordinaten Θ, φ von p' mit Θ', φ' und nehmen wir p' zum Pol eines neuen Polarsystems ω, ψ, so ist

$$\cos\omega = \cos\Theta\cos\Theta' + \sin\Theta\sin\Theta'\cos(\varphi-\varphi') = \lambda.$$

Da nun die Kugelfunktion P lediglich von ω, nicht aber von ψ abhängen soll, so ist (nach der Endformel des vorigen Artikels)

$$P = Const \cdot D^n(\lambda^2-1)^n.$$

Es bleibt also noch die Aufgabe zu lösen, die Koeffizienten α_s, β_s in der Identität

$$D^n(\lambda^2-1)^n = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi)\sin\Theta^s D^{n+s}(x^2-1)^n$$

als Funktionen von Θ', φ' zu bestimmen. Da nun die linke Seite eine ganze rationale Funktion von

$$\lambda = \cos\omega = \cos\Theta\cos\Theta' + \sin\Theta\sin\Theta'\cos(\varphi-\varphi'),$$

also symmetrisch in bezug auf Θ, φ und Θ', φ', und folglich auch in bezug auf Θ', φ' eine Kugelfunktion n^{ter} Ordnuug ist, so sieht man voraus, daß

$$D^n(\lambda^2-1)^n = \sum_0^n \gamma_s \sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s \cdot D^{n+s}(x'^2-1)^n \cos s(\varphi-\varphi')$$

sein muß, worin γ_s absolute Zahlenkoeffizienten bedeuten, welche allein noch zu bestimmen bleiben, und wo $x' = \cos\Theta'$ gesetzt ist.

7.

Statt diese Aufgabe durch die Bemerkung anzugreifen, daß die beiden partiellen Derivierten dieser Kugelfunktion, nach Θ und nach Θ' genommen, sich verhalten müssen, wie $\frac{d\lambda}{d\Theta}$ und $\frac{d\lambda}{d\Theta'}$, wodurch

man ebenfalls zum Ziele kommen würde, schlagen wir einen anderen Weg ein, indem wir zunächst mit den uns zu Gebote stehenden Hilfsmitteln den bekannten Satz beweisen, daß, wenn $Y = f(\Theta, \varphi)$ eine beliebige Kugelfunktion n^{ter} Ordnung bedeutet,

$$\int Y D^n(\lambda^2 - 1)^n \, d\sigma = \frac{4\pi}{2n+1} \cdot 2^n \Pi(n) \cdot Y'$$

ist, worin die Integration links über die ganze Kugelfläche auszudehnen, und $Y' = f(\Theta', \varphi')$ ist.

Zu dem Zwecke denken wir uns Y als Funktion von ω, ψ in die Form

$$Y = \sum_0^n (a_s \cos s\psi + b_s \sin s\psi) \sin^s \omega \cdot D^{n+s}(\lambda^2 - 1)^n$$

entwickelt, und zerlegen die Kugelfläche diesen Koordinaten ω, ψ gemäß in unendlich kleine Elemente $d\sigma = \sin\omega \, d\omega \, d\psi$; so erhalten wir

$$\int Y D^n(\lambda^2 - 1)^n d\sigma = \int_0^\pi D^n(\lambda^2 - 1)^n \sin\omega \, d\omega \int_0^{2\pi} Y \, d\psi$$

$$= \int_0^\pi D^n(\lambda^2 - 1)^n \sin\omega \, d\omega \cdot 2\pi \cdot a_0 \cdot D^n(\lambda^2 - 1)^n$$

$$= 2\pi a_0 \int_{-1}^{+1} [D^n(\lambda^2 - 1)^n]^2 \, d\lambda = \frac{4\pi}{2n+1} \cdot [2^n \Pi(n)]^2 \cdot a_0.$$

Setzen wir aber in der obigen Form für Y die Variable $\omega = 0$, also $\lambda = 1$, so wird $Y = f(\Theta', \varphi') = Y'$, und folglich (Art. 4)

$$Y' = a_0 \cdot D^n(\lambda^2 - 1)^n]_{\lambda=1} = a_0 h_0 = a_0 \cdot 2^n \Pi(n).$$

Wir erhalten daher

$$\int Y D^n(\lambda^2 - 1)^n d\sigma = \frac{4\pi}{2n+1} \cdot 2^n \Pi(n) \cdot Y';$$

was zu beweisen war.

Dieser Satz bildet die Ergänzung zu dem anderen Satze, daß, über die ganze Kugelfläche ausgedehnt,

$$\int ZY \, d\sigma = 0$$

ist, wenn Z und Y Kugelfunktionen von verschiedenen Ordnungen bedeuten. Dieses folgt unmittelbar aus der Gleichung (IV), wenn

man bedenkt, daß in diesem Falle das dort stehende Integral rechts wegfällt, und daß das zweite Integral links symmetrisch in bezug auf Y und Z ist; denn daraus folgt

$$n(n+1)\int ZY\,d\sigma = \int\left\{\frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta^2}\frac{dZ}{d\varphi}\frac{dY}{d\varphi}\right\}d\sigma = m(m+1)\int ZY\,d\sigma,$$

wenn m die Ordnung der Kugelfunktion Z ist. Wenn nun m und n verschieden sind, so ergibt sich unmittelbar der zuletzt aufgestellte Satz.

8.

Wir können nun leicht die Koeffizienten γ_s in der Entwicklung von $D^n(\lambda^2-1)^n$ in Art. 6 bestimmen, nach einem von Dirichlet angegebenen Verfahren. Setzen wir nämlich in dem ersten Satze des vorigen Artikels die spezielle Funktion

$$Y = \cos s\varphi \cdot \sin\Theta^s \cdot D^{n+s}(x^2-1)^n,$$

also

$$Y' = \cos s\varphi' \cdot \sin\Theta'^s \cdot D^{n+s}(x'^2-1)^n,$$

ein, so wird, wenn wir die Entwicklung von $D^n(\lambda^2-1)^n$ substituieren, die Kugelfläche, dem Polarsystem Θ, φ gemäß, in unendlich kleine Elemente $d\sigma = \sin\Theta\, d\Theta\, d\varphi$ zerlegen, und die Variabeln $x = \cos\Theta$ einführen,

$$\int YD^n(\lambda^2-1)^n d\sigma = \gamma_s \sin\Theta'^s D^{n+s}(x'^2-1)^n \cos s\varphi' \cdot \frac{2\pi}{2n+1}\cdot\frac{\Pi(n+s)}{\Pi(n-s)}[2^n\Pi(n)]^2$$

für ein von Null verschiedenes s, während für $s=0$ der doppelte Wert zu nehmen ist. Da nun dies Resultat mit

$$\frac{4\pi}{2n+1}\,2^n\Pi(n)Y' = \frac{4\pi}{2n+1}\cdot 2^n\Pi(n)\cdot\cos s\varphi'\cdot\sin\Theta'^s D^{n+s}(x'^2-1)^n$$

identisch sein muß, so folgt, wenn s von Null verschieden,

$$\gamma_s = 2\cdot\frac{1}{2^n\Pi(n)}\cdot\frac{\Pi(n-s)}{\Pi(n+s)},$$

dagegen

$$\gamma_0 = \frac{1}{2^n\Pi n}.$$

Folglich ist

$$D^n(\lambda^2-1)^n$$
$$= \frac{2}{2^n\Pi(n)}\sum_0^n\frac{\Pi(n-s)}{\Pi(n+s)}\cdot\sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s D^{n+s}(x'^2-1)^n\cos s(\varphi-\varphi'),$$

worin aber für $s = 0$ das entsprechende Glied auf die Hälfte zu reduzieren ist; diesen Übelstand vermeidet man in der Form

$$D^n(\lambda^2 - 1)^n$$
$$= \frac{1}{2^n \Pi(n)} \cdot \sum_{-n}^{+n} \frac{\Pi(n-s)}{\Pi(n+s)} \sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s D^{n+s}(x'^2-1)^n \cos s(\varphi-\varphi'),$$

die man leicht aus der vorhergehenden ableitet.

9.

Zum Schluß wollen wir noch den Zusammenhang der letzten Untersuchung mit gewissen Reihenentwicklungen bemerken.

Bezeichnet r die Entfernung eines Punktes, dessen rechtwinklige Koordinaten

$$\xi = \varrho \cos\Theta, \quad \eta = \varrho \sin\Theta \cos\varphi, \quad \zeta = \varrho \sin\Theta \sin\varphi$$

sind, von einem festen Punkte, so genügt bekanntlich die Funktion $v = \frac{1}{r}$ der partiellen Differentialgleichung (III) und folglich auch der Gleichung (II). Nehmen wir als festen Punkt einen Punkt der mit dem Radius $= 1$ beschriebenen Kugelfläche, dessen Koordinaten

$$\xi' = \cos\Theta', \quad \eta' = \sin\Theta' \cos\varphi', \quad \zeta' = \sin\Theta' \sin\varphi'$$

sind, so ist

$$r^2 = 1 - 2\lambda\varrho + \varrho^2,$$

worin

$$\lambda = \cos\omega = \cos\Theta \cos\Theta' + \sin\Theta \sin\Theta' \cos(\varphi - \varphi')$$

ist. Entwickelt man daher $\frac{1}{r}$ in eine unendliche Reihe:

$$\frac{1}{r} = \frac{1}{\sqrt{1 - 2\lambda\varrho + \varrho^2}} = \sum_0^\infty P_n(\lambda) \cdot \varrho^n, \quad \text{für } \varrho < 1,$$

worin $P_n(\lambda)$ eine rationale ganze Funktion von λ bezeichnet, so ist

$$\frac{1}{r} = \frac{\frac{1}{\varrho}}{\sqrt{1 - 2\lambda\frac{1}{\varrho} + \left(\frac{1}{\varrho}\right)^2}} = \sum_0^\infty \frac{P_n(\lambda)}{\varrho^{n+1}}, \quad \text{für } \varrho < 1,$$

und $P_n(\lambda)$ ist eine rationale ganze Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$, welche der partiellen Differentialgleichung (I) Genüge leistet, folglich eine Kugelfunktion n^{ter} Ordnung ist. Da sie aber

die Variabeln Θ, φ nur in der Form $\lambda = \cos\omega$ enthält, so ist (nach Art. 6)

$$P_n(\lambda) = Const \cdot D^n(\lambda^2 - 1)^n = k_n D^n(\lambda^2 - 1)^n,$$

worin nur noch die Konstante k_n zu bestimmen ist; diese ergibt sich für $\lambda = 1$; denn man erhält

$$P_n(1) = k_n \cdot h_0 = 2^n \Pi(n) \cdot k_n.$$

Andererseits ist $P_n(1)$ der Koeffizient von ϱ^n in der Entwicklung

$$\frac{1}{\sqrt{1 - 2\varrho + \varrho^2}} = \frac{1}{1 - \varrho} = \sum_0^\infty \varrho_n,$$

also

$$P_n(1) = 1, \quad \text{folglich} \quad k_n = \frac{1}{2^n \Pi(n)}$$

und

$$P_n(\lambda) = \frac{D^n(\lambda^2 - 1)^n}{2^n \Pi(n)}.$$

Mit Hilfe dieses Satzes kann man die vorletzte Gleichung des vorigen Artikels auch so schreiben:

$$P_n(\lambda) = 2 \sum_0^n \frac{\Pi(n-s)}{\Pi(n+s)} \cdot \sin\Theta^s D^s P_n(x) \cdot \sin\Theta'^s D^s P_n(x') \cdot \cos s(\varphi - \varphi'),$$

worin nur das $s = 0$ entsprechende Glied auf die Hälfte zu reduzieren ist. Ferner nimmt der Satz des Art. 7 die Gestalt

$$\int Y P_n(\lambda) \, d\sigma = \frac{4\pi}{2n + 1} \cdot Y'$$

an, in welcher er gewöhnlich geschrieben wird. Als spezieller Fall desselben ist bemerkenswert

$$\int P_n(\lambda) P_n(\mu) \, d\sigma = \frac{4\pi}{2n + 1} \cdot P_n(\nu),$$

worin

$$\lambda = \cos\omega = \cos\Theta \cos\Theta' + \sin\Theta \sin\Theta' \cos(\varphi - \varphi')$$
$$\mu = \cos\omega' = \cos\Theta \cos\Theta'' + \sin\Theta \sin\Theta'' \cos(\varphi - \varphi'')$$
$$\nu = \cos\omega'' = \cos\Theta' \cos\Theta'' + \sin\Theta' \sin\Theta'' \cos(\varphi' - \varphi'')$$

die Kosinus der drei Seiten eines sphärischen Dreiecks sind, dessen drei Ecken die beiden festen Punkte (Θ', φ'), (Θ'', φ'') und der bewegliche Punkt (Θ, φ) sind.

VIII.

Über Kreisevolventen.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1859, S. 363—365.]

Die Betrachtung der sukzessiven Evolventen des Kreises führt zu einer einfachen mechanischen Konstruktion der Glieder der Exponentialreihe, welche, soviel ich weiß, noch nicht bemerkt ist. Beschreibt man mit dem Radius r einen Kreis K_1 und wählt auf seiner Peripherie einen bestimmten Punkt m_0, von welchem aus der (in einem bestimmten Sinne positiv genommene) Drehungswinkel φ gerechnet wird, so ist das Stück der Peripherie von dem Punkte m_0 bis zu dem Punkte m_1, welcher dem Winkel φ entspricht,

$$m_0 m_1 = r\varphi.$$

Wickelt man dieses Stück ab, vom Punkte m_0 aus, so beschreibt m_0 ein Stück $m_0 m_2$ der Kreisevolvente K_2, welches

$$m_0 m_2 = \frac{r\varphi^2}{1 \cdot 2}$$

ist. Wickelt man abermals dies Stück ab, so daß die Ablösung des Fadens am Punkte m_0 beginnt, so beschreibt m_0 ein Stück

$$m_0 m_3 = \frac{r\varphi^3}{1 \cdot 2 \cdot 3}$$

der Evolvente K_3 der Kurve K_2, und so fort. Der Radius r und die Kurvenstücke $m_0 m_1$, $m_0 m_2$, $m_0 m_3$ ... bilden die sukzessiven Glieder der unendlichen Reihe, in welche re^{φ} entwickelt wird.

Der Beweis läßt sich am einfachsten durch Betrachtung der komplexen Größen und ihrer geometrischen Bedeutung führen, wie folgt.

Wir betrachten die beiden reellen Funktionen x_n und y_n der reellen Variabeln φ, welche durch die Gleichung

$$x_n + y_n i = re^{\varphi i} + \frac{r\varphi}{1} e^{\left(\varphi - \frac{\pi}{2}\right)i} + \cdots + \frac{r\varphi^{n-1}}{1 \cdot 2 \cdot 3 \cdots (n-1)} e^{\left(\varphi - (n-1)\frac{\pi}{2}\right)i}$$

definiert sind ($i = \sqrt{-1}$), als zusammengehörige rechtwinklige Koordinaten eines Punktes m_n einer Ebene; der Ort aller dieser Punkte, welche allen reellen Werten von φ entsprechen, bildet eine Kurve K_n; für $\varphi = 0$ erhält man den Punkt $x_n = r$, $y_n = 0$; wir wollen ihn mit m_0 bezeichnen und rechnen von ihm aus den Bogen $s_n = m_0 m_n$ der Kurve nach der Seite hin, welche positiven Werten von φ entspricht. Nun ist für $h \geqq 1$:

$$d\left(\frac{r\varphi^h}{1\cdot 2\cdots h} e^{\left(\varphi - h\frac{\pi}{2}\right)i}\right)$$

$$= \frac{r\varphi^{h-1}}{1\cdot 2\cdots(h-1)} e^{\left(\varphi - h\frac{\pi}{2}\right)i} d\varphi - \frac{r\varphi^h}{1\cdot 2\cdots h} e^{\left(\varphi - (h+1)\frac{\pi}{2}\right)i} d\varphi,$$

und

$$d(re^{\varphi i}) = -re^{\left(\varphi - \frac{\pi}{2}\right)i} d\varphi,$$

woraus sogleich durch paarweise Destruktion der Glieder

$$dx_n + i\,dy_n = -\frac{r\varphi^{n-1}}{1\cdot 2\cdots(n-1)} e^{\left(\varphi - n\frac{\pi}{2}\right)i} d\varphi;$$

$$ds_n = \frac{r\varphi^{n-1}d\varphi}{1\cdot 2\cdots(n-1)}; \quad s_n = \frac{r\varphi^n}{1\cdot 2\cdots n} = m_0 m_n$$

folgt; außerdem leuchtet ein, daß $t_n = \varphi - n\frac{\pi}{2}$ die Neigung der Tangente im Punkte m_n ist, in dem Sinne genommen, nach welchem φ und s_n abnehmen. Man kann daher die erste Gleichung so schreiben

$$x_n + y_n i = re^{\varphi i} + s_1 e^{t_1 i} + s_2 e^{t_2 i} + \cdots + s_{n-1} e^{t_{n-1} i}$$

oder

$$x_n + y_n i = x_{n-1} + y_{n-1} i + s_{n-1} e^{t_{n-1} i},$$

wodurch unmittelbar ausgedrückt ist, daß die Kurve K_n die Evolvente der Kurve K_{n-1} ist.

Für $n = 1$ erhält man die Gleichungen

$$x_1 = r\cos\varphi, \quad y_1 = r\sin\varphi$$

des Kreises K_1; für $n = 2$ die Gleichungen

$$x_2 = r\cos\varphi + r\varphi\sin\varphi, \quad y_2 = r\sin\varphi - r\varphi\cos\varphi$$

der Kreisevolvente K_2 usf.

Ich bemerke nur noch, daß man die allgemeine Gleichung auch so schreiben kann

$$x_n + y_n i = r e^{\varphi i}\left\{1 + \frac{-\varphi i}{1} + \frac{(-\varphi i)^2}{1\cdot 2} + \cdots + \frac{(-\varphi i)^{n-1}}{1\cdot 2\cdots(n-1)}\right\}$$
$$= r e^{\varphi i}[e^{-\varphi i}]_n,$$

wo der letzte Faktor auf der rechten Seite die Summe der ersten n Glieder der Entwicklung von $e^{-\varphi i}$ bedeutet. Mag φ noch so groß sein, so wird für unendlich wachsende Werte von n stets $lim\, s_n = 0$, $lim\,(x_n + y_n i) = r$, d. h. der Punkt m_n nähert sich unbegrenzt wieder dem Punkte m_0.

IX.

Über die Elemente der Wahrscheinlichkeitsrechnung.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 66—75.]

In den meisten Lehrbüchern findet man die Sätze über die sogenannten zusammengesetzten Wahrscheinlichkeiten in folgender Weise aufgestellt: „Ist a die Wahrscheinlichkeit eines Ereignisses A, b die eines zweiten B, so ist $a + b$ die Wahrscheinlichkeit, daß A oder B, und ab die Wahrscheinlichkeit, daß A und B eintritt". Man überzeugt sich aber leicht, daß von diesen beiden Sätzen immer höchstens einer richtig sein kann, und daß auch in unzähligen Fällen beide falsch sind. Dies findet seinen Grund darin, daß die Wahrscheinlichkeit eines zusammengesetzten Ereignisses durchaus nicht allein von den Wahrscheinlichkeiten der einzelnen Ereignisse, sondern außerdem noch von der gegenseitigen Beziehung derselben zueinander abhängt. Die so häufig vorkommende Vernachlässigung dieses Umstandes mag die nachfolgende Darstellung eines so elementaren Gegenstandes entschuldigen, auf welche in einer späteren Mitteilung Bezug genommen wird.

1.

Bei der ursprünglichen Begriffsbestimmung der mathematischen Wahrscheinlichkeit eines Ereignisses A muß man immer von der Voraussetzung ausgehen, daß sich gewisse Elementarfälle aufzählen lassen, welche die doppelte Bedingung erfüllen, erstens, daß einer, aber auch nur einer von ihnen eintreten muß; zweitens, daß wir keinen Grund haben, das Eintreten eines dieser Fälle eher zu erwarten als das eines anderen. Sind diese beiden Bedingungen erfüllt, und ist p die Anzahl derjenigen dieser Fälle, in welchen A eintritt, q die Anzahl der übrigen, so ist der Bruch $\frac{p}{p+q}$ das Maß für die Wahrscheinlichkeit, mit welcher wir das Eintreten des Ereignisses A erwarten. Ist dagegen eine der beiden Bedingungen nicht zu erfüllen, so bleibt eine genaue Schätzung der Wahrscheinlichkeit von A unmöglich.

Handelt es sich nun um Eintreten oder Nichteintreten von zwei Ereignissen A und B (deren Identität nicht ausgeschlossen ist), so

denken wir uns die sämtlichen Elementarfälle in vier Gruppen zerlegt; es sei nämlich die Anzahl aller Elementarfälle, in welchen

1. A und B eintritt, gleich m,
2. A allein eintritt, gleich p,
3. B allein eintritt, gleich q,
4. weder A noch B eintritt, gleich n.

Jeder Elementarfall gehört jedenfalls einer, aber auch nur einer dieser vier Gruppen an, so daß $m+p+q+n$ die Anzahl aller Elementarfälle ist. Zufolge der vorhergehenden Definition ist dann

$$a = \frac{m+p}{m+p+q+n}$$ die Wahrscheinlichkeit von A;

$$b = \frac{m+q}{m+p+q+n}$$ die Wahrscheinlichkeit von B.

Man sieht nun, daß die Wahrscheinlichkeit eines von dem Eintreten oder Nichteintreten von A und B abhängigen Ereignisses im allgemeinen von den drei Verhältnissen zwischen den vier Zahlen m, p, q, n abhängt, also durch alleinige Angabe der zwei Zahlen a, b noch nicht vollständig bestimmt ist. Es muß daher noch eine dritte Zahl, ein Element gegeben sein, welches dazu dient, die Art des Zusammenhanges zwischen den beiden Ereignissen A und B zu charakterisieren. Im allgemeinen wird nämlich das Eintreten eines dieser beiden Ereignisse die Wahrscheinlichkeit des andern abändern. Tritt z. B. das Ereignis B ein, so ist die Wahrscheinlichkeit von A — da dann die Fälle der zweiten und vierten Gruppe ausgeschlossen sind — jetzt

$$\alpha = \frac{m}{m+q};$$

und ähnlich ist die, durch die Gewißheit von A modifizierte Wahrscheinlichkeit von B

$$\beta = \frac{m}{m+p}.$$

Ist nun außer a und b noch eine der beiden modifizierten Wahrscheinlichkeiten α, β gegeben, so läßt sich die Wahrscheinlichkeit eines jeden aus A und B zusammengesetzten Ereignisses bestimmen. Zunächst muß zwischen den vier Zahlen a, b, α, β, welche nur von den Verhältnissen zwischen m, p, q, n abhängen, eine Relation bestehen; eliminiert man m, p, q, n, so erhält man

(1) $$a\beta = b\alpha,$$

und zwar ist der gemeinschaftliche Wert dieser beiden Produkte gleich

$$\frac{m}{m+p+q+n} = \omega;$$

also gleich der Wahrscheinlichkeit, daß A und B eintreten. Ferner ist die Wahrscheinlichkeit, daß A allein eintritt, gleich

$$(2) \qquad \frac{p}{m+p+q+n} = a - b\alpha = a(1-\beta) = a - \omega;$$

ebenso ist

$$(3) \qquad \frac{q}{m+p+q+n} = b(1-\alpha) = b - a\beta = b - \omega$$

die Wahrscheinlichkeit, daß B allein eintritt; und

$$(4) \qquad \frac{n}{m+p+q+n} = 1 - a - b + b\alpha$$
$$= 1 - a - b + a\beta = 1 - a - b + \omega$$

ist die Wahrscheinlichkeit, daß weder A noch B eintritt.

Ferner ist:

$$(5) \qquad \frac{m+n}{m+p+q+n} = 1 - a - b + 2\omega$$

die Wahrscheinlichkeit, daß keines der beiden Ereignisse A, B allein eintritt;

$$(6) \qquad \frac{m+p+q}{m+p+q+n} = a + b - b\alpha = a + b - a\beta = a + b - \omega$$

die, daß mindestens eins der beiden Ereignisse eintritt;

$$(7) \qquad \frac{p+q+n}{m+p+q+n} = 1 - b\alpha = 1 - a\beta = 1 - \omega$$

die, daß höchstens eins der beiden Ereignisse eintritt;

$$(8) \qquad \frac{m+q+n}{m+p+q+n} = 1 - a + b\alpha = 1 - a(1-\beta) = 1 - a + \omega$$

die, daß A nicht allein eintritt; und endlich ist

$$(9) \qquad \frac{m+p+n}{m+p+q+n} = 1 - b(1-\alpha) = 1 - b + a\beta = 1 - b + \omega$$

die Wahrscheinlichkeit, daß B nicht allein eintritt.

Um die Bedeutung von α, β noch anschaulicher zu machen, mögen hier noch folgende Bemerkungen Platz finden. Man sagt, zwei Ereignisse A und B schließen einander aus, wenn das Ein-

treten des einen das des andern unmöglich macht; der arithmetische Ausdruck dafür ist

$$\alpha = 0, \quad \beta = 0, \quad \omega = 0$$

(vorausgesetzt, daß a und b nicht selbst $= 0$ sind); dann ist die Wahrscheinlichkeit, daß mindestens eins der beiden Ereignisse eintritt, d. h. daß wirklich eins eintritt,

$$= a + b.$$

Man sagt ferner, zwei Ereignisse sind voneinander unabhängig, wenn das Eintreten des einen durchaus keinen Einfluß auf die Wahrscheinlichkeit des andern ausübt, d. h. wenn

$$\alpha = a, \quad \beta = b, \quad \omega = ab$$

ist; in diesem Falle ist die Wahrscheinlichkeit, daß mindestens eins der beiden Ereignisse eintritt,

$$= a + b - ab.$$

Und umgekehrt sieht man, daß der erste der beiden zu Anfang erwähnten Sätze nur dann richtig ist, wenn die beiden Ereignisse einander ausschließen, und der zweite nur dann, wenn sie voneinander unabhängig sind; und nur dann sind beide Sätze zu gleicher Zeit richtig, wenn mindestens eins der beiden Ereignisse unmöglich ist.

Ist ferner $\alpha = 1$, so zieht das Eintreten von B das von A als notwendige Folge nach sich, und dann ist $b = a\beta \gtrless a$. Ist außerdem $\beta = 1$, so ist $a = b$, und die beiden Ereignisse sind gewissermaßen identisch; aber es ist wohl zu bemerken, daß nicht umgekehrt aus $a = b$ diese Identität der Ereignisse folgt.

2.

Es hat nun keine Schwierigkeit, diese Sätze auf Kombinationen von mehr als zwei Ereignissen auszudehnen; sind z. B. $W_1, W_2, \ldots W_n$ Ereignisse, von denen je zwei einander ausschließen, und sind w_1, $w_2, \ldots w_n$ ihre Wahrscheinlichkeiten, so ist die Summe

$$w_1 + w_2 + \cdots + w_n$$

die Wahrscheinlichkeit, daß eins dieser Ereignisse eintritt, wovon man sich leicht durch den Schluß von n auf $(n + 1)$ überzeugt.

Man kann sich dieses Satzes häufig bedienen, um die Wahrscheinlichkeit a eines Ereignisses A zu bestimmen, ohne auf die Aufzählung der einzelnen gleich möglichen Elementarfälle zurück-

zugehen. Gesetzt, man habe verschiedene einander ausschließende Eventualitäten $B_1, B_2, \ldots B_n$, in welchen das Ereignis A eintreten kann, in so erschöpfender Weise aufgestellt, daß das Eintreten von A unter keiner anderen Eventualität möglich ist. Es sei b die Wahrscheinlichkeit, daß die Eventualität B_r eintritt, und α_r sei die Wahrscheinlichkeit, daß, wenn B_r eintritt, auch A eintritt. Dann ist

$$a = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n;$$

denn irgend ein Glied $b_r\alpha_r = w_r$ ist die Wahrscheinlichkeit des Ereignisses W_r, daß gleichzeitig B_r und A eintritt, und das Ereignis A ist identisch mit demjenigen, daß von diesen n einander ausschließenden Ereignissen $W_1 \ldots W_n$ irgend eins eintritt.

Umgekehrt kann man nun auch, wenn das Ereignis A wirklich eingetreten ist, die Wahrscheinlichkeit a posteriori bestimmen, daß dies infolge der Eventualität B_r geschehen ist; denn diese Wahrscheinlichkeit β_r ist nichts anderes, als die durch die Gewißheit von A modifizierte Wahrscheinlichkeit von B_r, so daß

$$a\beta_r = b_r\alpha_r, \quad \text{also} \quad \beta_r = \frac{b_r\alpha_r}{b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n},$$

und die hieraus sich ergebende Gleichung

$$\beta_1 + \beta_2 + \cdots + \beta_n = 1$$

ist nur ein Ausdruck für unsere ursprüngliche Annahme, daß das Eintreten von A nur unter einer der Eventualitäten $B_1, B_2, \ldots B_n$ und auch unter keiner anderen möglich ist. Von diesem Satze über die Wahrscheinlichkeit a posteriori wird in einer folgenden Mitteilung Gebrauch gemacht werden.

	1	2	3	4	x
1	(10)	(8)	(1)	(1)	
2	(8)	(9)	(7)	(6)	
3	(1)	(7)	(1)	(1)	
4	(1)	(6)	(1)	(2)	
y					

Ein Beispiel, welches zugleich zu einer weiteren Bemerkung Veranlassung geben wird, mag das Bisherige erläutern. Es seien

16 Urnen in quadratischer Anordnung aufgestellt, so daß sie vier Vertikalreihen ($x = 1, 2, 3, 4$) und vier Horizontalreihen ($y = 1, 2, 3, 4$) von je vier Urnen bilden; die einzelnen Urnen können dann durch Angabe der Vertikalreihe x und der Horizontalreihe y, in denen sie sich finden, voneinander unterschieden werden. In jeder Urne seien zehn Kugeln enthalten, von denen so viele weiß sind, wie die in Klammern gesetzte Zahl angibt (also enthält z. B. die Urne ($x = 1$, $y = 1$) nur weiße Kugeln, die Urne ($x = 4$, $y = 3$) enthält eine weiße und neun schwarze Kugeln). [*)] Wir nehmen an, daß der Zug ebensowohl aus der einen wie aus jeder anderen Urne geschehen kann; dann ist die Wahrscheinlichkeit, daß eine weiße Kugel gezogen wird

$$a = \Sigma b_{x,y}\, \alpha_{x,y} = \frac{1}{16} \Sigma \alpha_{x,y} = \frac{7}{16},$$

wo $b_{x,y}$ die Wahrscheinlichkeit $\frac{1}{16}$ bedeutet, daß der Zug aus der Urne (x, y) geschehen wird, und $\alpha_{x,y}$ die Wahrscheinlichkeit, daß der Zug, wenn er aus der Urne (x, y) geschieht, eine weiße Kugel geben wird.

Nun sei umgekehrt eine weiße Kugel gezogen, ohne daß man die Urne kennt, aus welcher sie gezogen ist. Dann ist die Wahrscheinlichkeit a posteriori, daß dieser Zug aus der Urne (x, y) geschehen ist,

$$\beta_{x,y} = \frac{b_{x,y}\, \alpha_{x,y}}{\Sigma b_{x,y}\, \alpha_{x,y}} = \frac{\alpha_{x,y}}{\Sigma \alpha_{x,y}} = \frac{\alpha_{x,y}}{7}.$$

Am wahrscheinlichsten ist es daher, daß der Zug aus der Urne (1, 1) geschehen ist; d. h. also, das wahrscheinlichste System der beiden Unbekannten x, y ist das System $x = 1$, $y = 1$.

Man findet nun häufig die ganz unrichtige Ansicht, daß der Wert einer unbekannten Größe, der ihr in dem wahrscheinlichsten System von mehreren Unbekannten zukommt, zugleich auch ihr wahrscheinlichster Wert sein müsse. Daß dem nicht so ist, lehrt recht augenfällig das vorliegende Beispiel; denn wir finden für die Wahrscheinlichkeit, daß der Zug aus der ersten, zweiten, dritten, vierten Vertikalreihe geschehen ist, d. h. daß x den Wert 1, 2, 3, 4 hat, resp. den Wert

$$\frac{2}{7}, \frac{3}{7}, \frac{1}{7}, \frac{1}{7};$$

[*) In der Originalarbeit ist die Tabelle über die Anzahlen weißer Kugeln nicht frei von Druckfehlern.]

und dieselben Zahlen drücken auch (infolge der Symmetrie des obigen Schemas) die Wahrscheinlichkeiten aus, daß die Unbekannte y den Wert 1, 2, 3 4 hat. Wir finden also, daß der wahrscheinlichste Wert von x gleich 2, der von y gleich 2 ist; und doch haben wir vorher gesehen, daß das wahrscheinlichste Wertsystem der beiden Unbekannten das System $x = 1$, $y = 1$ ist. Die Wichtigkeit dieser Bemerkung wird in einer späteren Mitteilung sich herausstellen.

Ganz ähnlich verhält es sich, wenn die Werte der unbekannten Größen ein Gebiet stetig erfüllen. Ist z. B.

$$\frac{1}{2\pi}(x^2 + 3y^2)e^{-(x^2+y^2)}\,dx\,dy$$

die Wahrscheinlichkeit, daß die Abszisse eines unbekannten Punktes in dem unendlich kleinen Intervall zwischen x und $x + dx$, und daß seine Ordinate zugleich zwischen y und $y + dy$ liegt, so findet man

$$\frac{1}{4\sqrt{\pi}}(2x^2 + 3)e^{-x^2}\,dx$$

als Wahrscheinlichkeit, daß seine Abszisse zwischen x und $x + dx$ liegt, und ebenso

$$\frac{1}{4\sqrt{\pi}}(6y^2 + 1)e^{-y^2}\,dy$$

als Wahrscheinlichkeit, daß seine Ordinate zwischen y und $y + dy$ liegt. Die erste Wahrscheinlichkeit wird ein Maximum für die beiden Systeme

$$x = 0, \quad y = \pm 1;$$

die zweite für den Wert

$$x = 0;$$

die dritte für die beiden Werte

$$y = \pm\sqrt{\frac{5}{6}}.$$

In diesem Falle stimmt das System der beiden wahrscheinlichsten Werte zwar sehr nahe, aber doch nicht vollständig mit dem wahrscheinlichsten Wertsystem überein.

X.

Über die Bestimmung der Präzision einer Beobachtungsmethode nach der Methode der kleinsten Quadrate.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 76—83.]

In seiner ersten Begründung der Methode der kleinsten Quadrate ging Gauß (Theoria motus corp. coel.) von der Voraussetzung aus, daß der wahrscheinlichste Wert einer beliebig oft auf dieselbe Weise direkt gemessenen Größe das arithmetische Mittel aus den durch diese Messungen erhaltenen Werten ist, und kam auf diese Weise zu dem Ausdruck

$$\frac{h}{\sqrt{\pi}} e^{-h^2 t^2} dt$$

für die Wahrscheinlichkeit, daß ein Beobachtungsfehler seinem Werte nach in dem unendlich kleinen Intervall zwischen t und $t + dt$ liegt; in diesem Ausdruck bedeutet h eine positive Konstante, welche für verschiedene Beobachtungsmethoden im allgemeinen auch verschiedene Werte hat, und zwar leuchtet ein, daß eine Beobachtungsmethode desto zuverlässiger ist, je größer der Wert der ihr zugehörigen Konstante h ist; denn die Wahrscheinlichkeit

$$\frac{h}{\sqrt{\pi}} \int_{-a}^{+a} e^{-h^2 t^2} dt = \frac{1}{\sqrt{\pi}} \int_{-ha}^{+ha} e^{-u^2} du$$

dafür, daß ein Fehler seinem absoluten Werte nach die positive Größe a nicht überschreitet, ist desto größer, je größer h ist. Aus diesem Grunde hat Gauß die Größe h die Präzision der Beobachtungsmethode genannt; in einer späteren Abhandlung (Zeitschrift für Astronomie usw. von Lindenau und Bohnenberger, Bd. I, 1816) hat er ferner gezeigt, wie man den wahrscheinlichsten Wert der Präzision einer Beobachtungsmethode bestimmen kann, wenn eine Reihe wirklich gemachter Beobachtungsfehler bekannt ist. Es wird für das Folgende nützlich sein, hier den von Gauß zu diesem Zwecke eingeschlagenen Weg wieder in Erinnerung zu bringen, welcher auf dem Satze über die Wahrscheinlichkeit a posteriori beruht.

Ist h die wahre Präzision der Beobachtungsmethode, so ist die Wahrscheinlichkeit, daß bei m aufeinanderfolgenden Beobachtungen die Fehler

$$t_1,\ t_2,\ \ldots,\ t_m$$

gemacht werden, gleich

$$\alpha = \left(\frac{h}{\sqrt{\pi}}\right)^m e^{-h^2 S} dt_1 dt_2 \ldots dt_m,$$

worin zur Abkürzung

$$S = t_1^2 + t_2^2 + \cdots + t_m^2$$

gesetzt ist. A priori, d. h. ehe irgend eine Messung vorgenommen ist, haben wir keinen Grund, der Präzision einer uns unbekannten Beobachtungsmethode einen Wert h eher beizulegen als einen anderen; folglich ist a posteriori, d. h. nachdem wirklich die Beobachtungsfehler $t_1, t_2, \ldots t_m$ gemacht sind, die Wahrscheinlichkeit der Hypothese, daß h der wahre Wert der Präzision ist, proportional dem α, also proportional dem Ausdruck

$$h^m e^{-h^2 S},$$

welcher für

$$\frac{1}{2h^2} = \frac{S}{m}, \quad \text{also} \quad h = \sqrt{\frac{m}{2S}}$$

ein Maximum wird; es ist also dies der wahrscheinlichste Wert der Präzision der Beobachtungsmethode.

In allen wirklichen Fällen liegt aber die Sache ganz anders. Die Objekte der Beobachtungen sind lineare Funktionen

$$v_1,\ v_2,\ \ldots\ v_m$$

von gewissen unbekannten Größen $x, y, z \ldots$, deren Anzahl n höchstens gleich der Anzahl m der Beobachtungen und deren Wertbestimmung gerade der Zweck dieser Beobachtungen ist. Sind nun

$$k_1,\ k_2,\ \ldots\ k_m$$

die durch die Beobachtungen gelieferten Werte von $v_1, v_2, \ldots v_m$, so bestimmt die aus dem obigen Wahrscheinlichkeitsgesetz eines beliebigen Fehlers t gefolgerte Methode der kleinsten Quadrate die Werte der Unbekannten $x, y, z \ldots$ durch die Forderung, daß die Quadratsumme

$$(k_1 - v_1)^2 + (k_2 - v_2)^2 + \cdots + (k_m - v_m)^2 = \Omega$$

ein Minimum werden soll. Wären nun diese wirklich die wahren Werte der Unbekannten, so wären die entsprechenden Werte der Differenzen

$$k_1 - v_1,\ k_2 - v_2,\ \ldots\ k_m - v_m$$

auch die wahren Beobachtungsfehler, und man könnte versucht sein, den wahrscheinlichsten Wert der Präzision h nach der früheren Regel zu bestimmen, indem man statt S nur das Minimum Ω_0 der Funktion Ω zu substituieren brauchte, so daß also

$$\sqrt{\frac{m}{2\,\Omega_0}}$$

als wahrscheinlichster Wert von h anzusehen wäre. Daß diese Formel aber nicht richtig sein kann, bemerkt man am deutlichsten in dem Falle, wo $n = m$ ist; dann können nämlich die gemachten Beobachtungen sämtlich durch ein und dasselbe Wertsystem $x, y, z, \ldots$ befriedigt werden, Ω_0 ist $= 0$, und man würde $h = \infty$, also das Resultat erhalten, daß die Beobachtungsmethode höchstwahrscheinlich absolut genau ist, während doch erst dann ein Urteil über die Präzision gestattet ist, wenn ein Überschuß von Beobachtungen vorliegt.

In einer späteren Abhandlung (Theoria combinationis etc. art. 39) in welcher das Prinzip des arithmetischen Mittels und damit zugleich das obige Wahrscheinlichkeitsgesetz eines Fehlers t ganz verlassen ist, hat Gauß für eine ähnliche Frage (die nach dem wahrscheinlichsten Werte des sogenannten mittleren Fehlers) die richtige Antwort gegeben, welche, auf die frühere Darstellungsweise übertragen, den Ausdruck

$$\sqrt{\frac{m-n}{2\,\Omega_0}}$$

als wahrscheinlichsten Wert der Präzision h liefert, so daß also das Minimum Ω_0 als eine Summe von nur $(m-n)$ Fehlerquadraten zu behandeln ist. Man sieht, daß diese Formel in dem Falle $n = m$ unter die ganz unbestimmte Form $\frac{0}{0}$ tritt, und in der Tat ist in diesem Falle gar kein Schluß auf die Präzision gestattet.

Es erscheint nun wünschenswert, einen Beweis dieses Satzes auch aus dem obigen Wahrscheinlichkeitsgesetz abzuleiten, da dies meines Wissens in befriedigender Weise noch nicht geschehen ist*). Dazu führt folgender einfache Weg.

---

*) So z. B. geht Wittstein (Anhang zu der Übersetzung von Naviers Differentialrechnung) von dem unrichtigen Satze aus, daß, wenn h die wahre Präzision ist, der wahrscheinlichste Wert eines Fehlerquadrates $= \frac{1}{2h^2}$, statt 0 ist.

In der Hypothese B, daß h, x, y, z, ... die wahren Werte der Präzision, der ersten, zweiten, dritten usw. Unbekannten sind, ist die Wahrscheinlichkeit, daß für die Funktionen

$$v_1,\ v_2,\ \ldots\ v_m$$

die Werte

$$k_1,\ k_2,\ \ldots\ k_m$$

durch Beobachtung geliefert, daß also die Beobachtungsfehler

$$k_1 - v_1,\ \ k_2 - v_2,\ \ \ldots\ \ k_m - v_m$$

gemacht werden, proportional dem Ausdruck

$$h^m e^{-h^2\Omega};$$

da nun alle denkbaren Hypothesen B a priori gleich wahrscheinlich sind, so ist a posteriori, d. h. nachdem wirklich die Werte $k_1, k_2, \ldots k_m$ beobachtet sind, die Wahrscheinlichkeit der Hypothese B proportional demselben Ausdruck; dieselbe ist daher

$$= C h^m e^{-h^2\Omega}\, dh\, dx\, dy\, dz \ldots,$$

worin

$$\frac{1}{C} = \int_0^{\infty} dh \int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dy \int_{-\infty}^{+\infty} dz \ldots h^m e^{-h^2\Omega}.$$

Fragt man nun nach dem wahrscheinlichsten Wertsystem von h, x, y, z, ..., so würde man untersuchen müssen, für welche Werte h, x, y, z, ... der Ausdruck

$$h^m e^{-h^2\Omega}$$

ein Maximum wird. Allein wir fragen nach dem wahrscheinlichsten Werte der Präzision allein; wir haben daher zunächst den Ausdruck der Wahrscheinlichkeit herzustellen, daß der Wert der Präzision zwischen h und $h + dh$ liegt. Diesen erhält man aus dem Vorhergehenden durch Integration über alle reellen Werte von x, y, z, ... Es ist aber nach bekannten Sätzen

$$\int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dy \int_{-\infty}^{+\infty} dz \ldots e^{-h^2\Omega} = K \frac{1}{h^n} e^{-h^2\Omega_0},$$

worin K von h unabhängig ist; folglich ist das aus den gemachten Beobachtungen resultierende Wahrscheinlichkeitsgesetz für die Präzision von der Form

$$H . h^{m-n} e^{-h^2\Omega_0} dh,$$

worin

$$\frac{1}{H} = \int_0^\infty h^{m-n} e^{-h^2 \Omega_0} dh$$

ist. Vergleicht man diese Form mit der früheren

$$H' h^m e^{-h^2 S} dh, \quad \text{wo} \quad \frac{1}{H'} = \int_0^\infty h^m e^{-h^2 S} dh,$$

welche sich ergab, wenn m wahre Beobachtungsfehler vorlagen, deren Quadratsumme $= S$ war, so findet man in der Tat vollständige Übereinstimmung, wenn man das Minimum Ω_0 der Summe von m Fehlerquadraten wie eine Summe von $m - n$ wirklichen Fehlerquadraten ansieht. Der wahrscheinlichste Wert zu der Präzision ist daher wirklich

$$= \sqrt{\frac{m-n}{2\Omega_0}}.$$

Hiermit ist der eigentliche Gegenstand dieser Mitteilung beendigt; zum Schluß mag noch folgende Bemerkung gemacht werden. Wir haben als wahrscheinlichsten Wert h einen anderen gefunden, als denjenigen, welcher dem h in dem wahrscheinlichsten System von Werten $h, x, y, z, \ldots$ zukommt. Man könnte nun befürchten, daß auch die Bestimmung der wahrscheinlichsten Werte von $x, y, z, \ldots$, wenn sie nach demselben Prinzip ausgeführt, wenn also für jede einzelne Unbekannte besonders der wahrscheinlichste Wert aufgesucht würde, von der durch die Methode der kleinsten Quadrate geforderten Regel abweichen könnte. Allein man überzeugt sich leicht, daß diese Befürchtung ungegründet ist, und daß das System der wahrscheinlichsten Werte von $x, y, z, \ldots$ übereinstimmt mit dem wahrscheinlichsten Wertsystem dieser Unbekannten.

Das letztere ist offenbar dasjenige, für welches die Quadratsumme Ω ein Minimum wird, und darin besteht ja gerade der Hauptsatz der Methode der kleinsten Quadrate; die entsprechenden Werte der n Unbekannten $x, y, z, \ldots$ findet man bekanntlich dadurch, daß man, was immer möglich ist, die Funktion Ω auf die Form

$$\Omega = Y^2 + Z^2 + \cdots + X^2 + \Omega_0$$

bringt, worin Y eine lineare Funktion aller n Unbekannten ist, die dadurch bestimmt wird, daß $\Omega - Y^2$ unabhängig von y wird; ähnlich

ist Z eine lineare Funktion der übrigen $(n-1)$ Unbekannten, und dadurch bestimmt, daß $\Omega - Y^2 - Z^2$ unabhängig von y, z wird, usf., so daß endlich X eine lineare Funktion von der n^{ten} Unbekannten x allein ist. Die Werte, welche Ω zu einem Minimum machen, sind diejenigen, welche die n Gleichungen

$$X = 0, \quad \ldots \quad Z = 0, \quad Y = 0$$

befriedigen, und das letzte Glied Ω_0 in dieser Form stellt offenbar den Minimumwert von Ω dar.

Fragt man nun aber nach dem wahrscheinlichsten Wert der Unbekannten x allein, so hat man zunächst den Ausdruck der Wahrscheinlichkeit abzuleiten, daß der Wert dieser Unbekannten zwischen den Grenzen x und $x + dx$ enthalten ist. Diesen erhält man durch Integration des obigen Wertes

$$C h^m e^{-h^2 \Omega} dh\, dx\, dy\, dz \ldots$$

in bezug auf alle zulässigen Werte der Unbekannten h, y, z, ... Bringt man die Summe Ω auf die oben erwähnte Form, so gibt die sukzessive Integration in bezug auf die $(n-1)$ Unbekannten y, z, ... ein Resultat

$$C' h^{m-n+1} e^{-h^2 (X^2 + \Omega_0)} dh\, dx,$$

worin C' unabhängig von h und x ist; integriert man endlich noch in bezug auf h, so erhält man für die gesuchte Wahrscheinlichkeit den Ausdruck

$$\frac{c\, dx}{(X^2 + \Omega_0)^{\frac{m-n+2}{2}}},$$

worin

$$\frac{1}{c} = \int_{-\infty}^{+\infty} \frac{dx}{(X^2 + \Omega_0)^{\frac{m-n+2}{2}}};$$

und hieraus folgt, daß derjenige Wert von x, für welchen $X = 0$ wird, unter allen der wahrscheinlichste ist. Dieser Wert stimmt daher wirklich mit dem durch die Methode der kleinsten Quadrate erhaltenen überein.

XI.

Zur Theorie der Maxima und Minima.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 84—88.]

In den Elementen der Differentialrechnung wird folgender Satz bewiesen:

„Sind innerhalb eines gewissen Wertengebietes der unabhängigen Variabeln x, y, z, ... die partiellen Derivierten erster Ordnung

$$\frac{du}{dx}, \quad \frac{du}{dy}, \quad \frac{du}{dz}, \quad \ldots$$

einer Funktion u dieser Variabeln überall endlich und stetig, so kann ein Maximum oder Minimum von u nur da eintreten, wo diese Derivierten sämtlich verschwinden."

Hat nämlich z. B. $\frac{du}{dx}$ einen von Null verschiedenen Wert, so erleidet u, wenn man der Variabeln x zwei beliebig kleine Änderungen von entgegengesetzten Vorzeichen gibt, ebenfalls Änderungen von entgegengesetzten Vorzeichen, so daß der entsprechende Wert von u weder ein Maximum noch ein Minimum sein kann.

Man bedient sich dieses Satzes, um die Stellen x, y, z, ... aufzusuchen, wo die Funktion ein Maximum oder Minimum wird; aber dies kann auch an solchen Stellen eintreten, wo die partiellen Derivierten unstetig werden, und zwar bietet sich dieser Fall häufig in ganz einfachen Aufgaben dar, wofür das folgende Beispiel einen Beleg geben mag, bei welchem diese Erscheinung bis jetzt unbeachtet geblieben ist.

Aufgabe: Es sind drei Punkte m_1, m_2, m_3 gegeben; es soll ein vierter Punkt m gefunden werden, für welchen die Summe der absoluten Distanzen mm_1, mm_2, mm_3 so klein wie möglich ausfällt.

Auflösung. Man nehme willkürlich im Raume ein rechtwinkliges Koordinatensystem, nenne x, y, z die Koordinaten des gesuchten

Punktes m, und r_1, r_2, r_3 die absoluten Werte seiner Distanzen von den drei gegebenen Punkten m_1, m_2, m_3, so daß

$$u = r_1 + r_2 + r_3$$

die Funktion von x, y, z ist, deren Minimumwert bestimmt werden soll. Verfährt man nun nach der gewöhnlichen Regel, so hat man

$$\frac{dr_1}{dx} + \frac{dr_2}{dx} + \frac{dr_3}{dx} = 0, \quad \frac{dr_1}{dy} + \frac{dr_2}{dy} + \frac{dr_3}{dy} = 0,$$
$$\frac{dr_1}{dz} + \frac{dr_2}{dz} + \frac{dr_3}{dz} = 0$$

zu setzen. Da man aber die Achsen mit jeder beliebigen Richtung h zusammenfallen lassen kann, so lassen sich diese drei Gleichungen in die einzige

$$\cos(p_1 h) + \cos(p_2 h) + \cos(p_3 h) = 0$$

zusammenfassen, in welcher p_1, p_2, p_3 die vom Punkte m nach m_1, m_2, m_3 laufenden Richtungen, und $(p_1 h)$, $(p_2 h)$, $(p_3 h)$ die Winkel bedeuten, welche dieselben mit der willkürlichen Richtung h einschließen.

Nimmt man h senkrecht auf p_2 und p_3, so folgt, daß h auch senkrecht auf p_1 ist, daß also die drei Richtungen p_1, p_2, p_3 und folglich auch die vier Punkte m, m_1, m_2, m_3 in einer Ebene liegen, was sich ohnehin erwarten ließ.

Läßt man ferner h sukzessive mit p_1, p_2, p_3 zusammenfallen, so erhält man

$$1 + \cos(p_2 p_1) + \cos(p_3 p_1) = 0,$$
$$\cos(p_1 p_2) + 1 + \cos(p_3 p_2) = 0,$$
$$\cos(p_1 p_3) + \cos(p_2 p_3) + 1 = 0,$$

woraus

$$\cos(p_2 p_3) = \cos(p_3 p_1) = \cos(p_1 p_2) = -\tfrac{1}{2}$$
$$(p_2 p_3) = (p_3 p_1) = (p_1 p_2) = 120^0$$

folgt.

Man erhält daher die bekannte Antwort, daß der Punkt m in der Ebene der drei Punkte m_1, m_2, m_3 so zu konstruieren ist, daß je zwei der drei Richtungen mm_1, mm_2, mm_3 einen Winkel von 120^0 miteinander bilden. Diese Konstruktion ist auch stets möglich, und liefert einen vollständig bestimmten Punkt m, sobald keiner der drei Winkel des Dreiecks $m_1 m_2 m_3$ größer ist als 120^0.

Ist aber einer der drei Winkel des Dreiecks $m_1 m_2 m_3$ größer als 120^0, so wird diese Konstruktion unausführbar; es gibt dann

keinen Punkt m von der Beschaffenheit, daß je zwei der drei Richtungen mm_1, mm_2, mm_3 einen Winkel von 120° bilden; es gibt also keinen Punkt m, für welchen die partiellen Derivierten der Funktion u gleichzeitig verschwinden. Andererseits leuchtet aber aus dem Begriff der Funktion u, welche stets positiv ist und für unendlich entfernte Punkte unendlich wächst, unmittelbar ein, daß sie irgendwo in endlicher Entfernung doch einen Minimumwert haben muß. Wir müssen daraus schließen, daß dieser Minimumwert an einer solchen Stelle eintritt, wo die partiellen Derivierten von u unstetig werden. Da nun die Derivierten der absoluten Distanz eines beliebigen Punktes von einem festen Punkte nur in diesem letzteren selbst unstetig werden, und u eine Summe von drei solchen absoluten Distanzen ist, so werden die Derivierten nur in den drei gegebenen Punkten m_1, m_2, m_3 unstetig; es muß daher der gesuchte Punkt m mit einem dieser drei Punkte zusammenfallen. Da endlich für den Fall, daß der Dreieckswinkel bei m_1 um unendlich wenig kleiner als 120° ist, die frühere Konstruktion den gesuchten Punkt m unendlich nahe bei m_1 liefert, und auch, wenn dieser Winkel $= 180°$ ist, der gesuchte Punkt offenbar mit m_1 zusammenfällt, so wird es daher so gut wie gewiß, daß auch für alle Werte des Winkels zwischen 120° und 180° die Spitze desselben der gesuchte Punkt ist.

Dies bestätigt sich analytisch, wenn man die unendlich kleine Änderung der Funktion u untersucht für den Fall, daß der variable Punkt m sich unendlich wenig von dem Punkte m_1 entfernt. Zieht man nämlich vom Punkte m_1 aus eine beliebige Richtung h, welche mit m_1m_2 und m_1m_3 die Winkel α und β einschließt, so ist die in dieser Richtung h genommene Derivierte der Funktion u gleich

$$1 - \cos\alpha - \cos\beta = 1 - 2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2};$$

bezeichnet man ferner mit Θ den Winkel zwischen den Richtungen m_1m_2 und m_1m_3, von dem wir annehmen, daß er zwischen 120° und 180° liegt, so folgt aus den bekannten Eigenschaften

$$\alpha + \beta + \Theta \leqq 360°, \quad \alpha + \beta \gtreqless \Theta,$$

der drei Winkel zwischen drei Richtungen, daß

$$120° \geqq \frac{\alpha+\beta}{2} \geqq 60°,$$

also

$$-\frac{1}{2} \leqq \cos\frac{\alpha+\beta}{2} \leqq +\frac{1}{2},$$

daß also der absolute Wert von $2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$ ein echter Bruch ist. Mithin ist die obige Derivierte stets positiv, und folglich wächst u von dem Punkte m_1 aus nach allen Richtungen hin, was zu beweisen war.

Da der absolute Wert der Differenz $\alpha - \beta \leqq \Theta$, also $\cos\frac{\alpha-\beta}{2}$ positiv ist, so kann die obige Derivierte nur dann den Wert Null haben, wenn

$$\cos\frac{\alpha-\beta}{2} = 1; \quad \cos\frac{\alpha+\beta}{2} = +\frac{1}{2}$$

ist, d. h. wenn

$$\alpha = \beta = 60^0 \quad \text{und folglich auch} \quad \Theta = 120^0,$$

also h die Halbierungsrichtung zwischen $m_1 m_2$ und $m_1 m_3$ ist. Aber in diesem Falle überzeugt man sich leicht, daß die zweite in derselben Richtung genommene Derivierte einen positiven Wert hat.

XII.

Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers.

[Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß, Braunschweig 1877, S. 1—55.]

Die erhabenen Schöpfungen von Carl Friedrich Gauß haben die Bewunderung der Mathematiker dieses Jahrhunderts vor allem deshalb erregt, weil sie in fast beispielloser Weise die Wissenschaft mit einer außerordentlichen Fülle ganz neuer Gedanken befruchtet und vorher gänzlich unbekannte Felder zum ersten Male der Forschung erschlossen haben. Im höchsten Maße gilt dies von Gauß' Entdeckungen im Gebiete der höheren Arithmetik, die ihn nach seinem eigenen Ausspruche das ganze Leben hindurch vor allen anderen Teilen der Mathematik gefesselt hat. Mit der Theorie der Kreisteilung ist von ihm nicht bloß der Grund zu einem neuen Teile der Mathematik gelegt, welcher von der algebraischen Verwandtschaft der Zahlen handelt, sondern sie hat auch das erste und bis jetzt noch immer fruchtbarste Beispiel des innigen Zusammenhangs zwischen der höheren Algebra und der Zahlentheorie geliefert, welche bis dahin zwei vollständig getrennte Gebiete gebildet hatten. In der nächsten Beziehung zu dieser Erweiterung der Grenzen der Wissenschaft steht der kühne Gedanke, den Begriff der ganzen Zahl durch die Einführung der ganzen komplexen Zahlen von seiner bisherigen Beschränkung zu befreien, wodurch Gauß abermals der arithmetischen Forschung ein heute noch unermeßliches Feld eröffnet hat. Aber es ist nicht bloß dieser wunderbare Reichtum an neuen Gedanken und großen Entdeckungen, durch welchen Gauß sein Wirken auf allen von ihm beschrittenen Gebieten der Wissenschaft für alle Zeiten bezeichnet hat, sondern es steht diesem vollständig ebenbürtig die Tiefe der Methoden gegenüber, durch welche er die größten Schwierig-

keiten überwunden und die verborgensten Wahrheiten, die *mysteria numerorum*, in das hellste Licht gesetzt hat. Es genügte seinem stets auf das Große und auf die zukünftige Entwicklung der Wissenschaft blickenden Geiste nicht, einen Beweis gefunden und damit die Wahrheit außer Zweifel gesetzt zu haben, sondern er kehrte, wie er selbst so eindringlich beschreibt, unablässig zu den schon überwundenen Schwierigkeiten zurück, in der Hoffnung, durch erneute Anstrengungen neue Waffen zu gewinnen, welche eine über das unmittelbar vorliegende Ziel weit hinausreichende Tragweite besäßen. Und so ist es gekommen, daß dieselben von Gauß erdachten Methoden unmittelbar oder mit geringen Modifikationen auch bei der Behandlung von ähnlichen, aber allgemeineren Problemen sich als vollständig ausreichend erweisen. Diese schon oft als ein besonders charakteristisches Kennzeichen der Gedankentiefe von Gauß hervorgehobene Erscheinung an einem neuen Beispiel zu bestätigen, ist der Zweck der gegenwärtigen Abhandlung, welche dem Andenken des großen Mathematikers gewidmet ist.

Die Theorie der binären quadratischen Formen, zu deren Entstehung einige Sätze von Fermat die Veranlassung gegeben haben verdankt ihre Begründung den hervorragenden Arbeiten von Euler und Lagrange, aber sie ist erst von Gauß durch die in der fünften Sektion der Disquisitiones Arithmeticae niedergelegten Untersuchungen zu einem wissenschaftlichen Ganzen gestaltet, und namentlich hat sie durch die daselbst zum ersten Male behandelte Lehre von der Komposition der Formen die höchste Bereicherung erhalten. Unter den Anwendungen, welche Gauß von dieser neuen Theorie gemacht hat, ist eine der bemerkenswertesten die Bestimmung des Verhältnisses der Klassen-Anzahlen der Formen, welche zu zwei verschiedenen Ordnungen derselben Determinante D gehören; bezeichnet man mit $h(D)$ die Klassen-Anzahl für diejenige Ordnung der Determinante D, welche nur primitive Formen (und zwar entweder nur die eigentlichen oder nur die uneigentlichen) enthält, so kommt diese Aufgabe darauf hinaus, für zwei gegebene, in quadratischem Verhältnis stehende Determinanten D und D' das Verhältnis $h(D):h(D')$ zu ermitteln. Die aus der Theorie der Komposition der Formen geschöpfte Beantwortung dieser Frage ist im Art. 256, V. und VI. enthalten, und sie ist für den Fall negativer Determinanten eine so vollständige, daß der Wert des Verhältnisses $h(D):h(D')$ unmittelbar

aus den Werten von D und D' entnommen werden kann; nicht ebenso vollständig durchgeführt ist der Fall positiver Determinanten, über welchen Gauß folgendes sagt: *„Pro casu tertio autem, ubi D est numerus positivus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitivarum in V, V', V'' etc. cum multitudine classium diversarum inde resultantium hucusque non habemus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi tt — Duu = AA satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (ut in casibus praecc.), de hac re nihil certi pronunciare possumus.“*

Das umfassendere und noch viel schwierigere Problem, die Klassen-Anzahl $h(D)$ selbst, d. h. die Abhängigkeit dieser Anzahl von der Determinante D zu bestimmen, ist schon während des Druckes der fünften Sektion der Disquisitiones Arithmeticae, wie aus Art. 306, X. hervorgeht, ein Gegenstand des höchsten Interesses für Gauß gewesen, und es ist ihm in der Tat bald darauf gelungen, die vollständige Lösung desselben zu finden, was er noch am Schlusse des großen Werkes mit folgenden Worten ankündigen konnte: *„Quaestionem hic propositam plene solvere nuper successit, quam disquisitionem plures partes tum Arithmeticae sublimioris tum Analyseos mirifice illustrantem in continuatione hujus operis trademus quam primum licebit.“* Allein die hier in Aussicht gestellte Veröffentlichung dieser Untersuchung ist zu Gauß' Lebzeiten nicht erfolgt; der hierauf bezügliche Teil seines Nachlasses, welchen ich in dem 1863 erschienenen zweiten Bande seiner gesammelten Werke herausgegeben habe, enthält namentlich zwei Fragmente, die aus den Jahren 1834 und 1837 stammen und den gemeinsamen Titel führen: *„De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem.“* Obgleich jedes dieser Fragmente nach wenigen Seiten abbricht, so reicht ihr Inhalt doch aus, um den Weg vollständig überblicken zu lassen, auf welchem Gauß zu dem erstrebten Ziele gelangt ist.

Im Jahre 1839, also 38 Jahre nach dem Erscheinen der Disquisitiones Arithmeticae, trat Peter Gustav Lejeune Dirichlet,

der nach Gauß' eigenem Zeugnis zuerst von allen Mathematikern dieses Werk vollständig begriffen und die darin enthaltenen Untersuchungen selbständig weitergeführt hat, mit einer vollständigen und höchst eigentümlichen Lösung des Problems der Klassen-Anzahl hervor*). Ohne hier, was zu weit führen würde, auf eine nähere Vergleichung der Methode von Dirichlet mit derjenigen von Gauß einzugehen, bemerke ich nur, daß von beiden für die Klassen-Anzahl ein Ausdruck durch eine unendliche Reihe gewonnen wird, welche sich mit Hilfe gewisser, der Kreisteilung angehörender Sätze von Gauß summieren, also in geschlossener Form darstellen läßt. Aber es ist von Wichtigkeit, daß es schon vor Ausführung dieser Summation gelingt, aus dem erhaltenen Ausdruck den Wert des oben besprochenen Verhältnisses $h(D):h(D')$ abzuleiten. Auf diese Weise**) ist Dirichlet für den Fall negativer Determinanten zu demselben Resultat gelangt wie Gauß, und er hat außerdem für den Fall positiver Determinanten zum ersten Male das Gesetz vollständig ausgesprochen, nach welchem das gesuchte Verhältnis von den kleinsten Lösungen der unbestimmten Gleichungen $tt - Duu = 1$, $t't' - D'u'u' = 1$ abhängt. Aus der oben angeführten, auf diesen Fall bezüglichen Stelle der Disquisitiones Arithmeticae geht aber wohl mit Gewißheit hervor, daß Gauß ebenfalls dieses Gesetz schon vollständig gekannt hat, welches zwar einfach, aber doch keineswegs so einfach ist, daß man *ex sola inspectione numerorum* D, D' den Wert des gesuchten Verhältnisses erkennen könnte; auch habe ich gezeigt***), daß man wirklich auf dem von Gauß eingeschlagenen Wege, d. h. durch die Komposition der Formen, mit wenigen Schritten zu diesem, zuerst von Dirichlet ausgesprochenen Gesetz gelangen kann.

Beide Methoden, das Verhältnis der Klassen-Anzahlen zu bestimmen, sowohl die von Gauß, welche auf die Komposition der Formen gegründet ist, als auch diejenige von Dirichlet, zeichnen sich nun dadurch aus, daß sie auf ähnliche Probleme von sehr allgemeinem Charakter mit demselben Erfolg anwendbar

---

*) Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Crelles Journal, Bd. 19, 21).

**) Ebenda, Bd. 21, § 8.

***) Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Zweite Auflage. 1871. §. 150, 151. — Ich werde dieses Werk in der Folge kurz mit D. zitieren.

sind*). Die binären quadratischen Formen, von welchen bisher ausschließlich gesprochen ist, bilden nämlich nur einen äußerst speziellen Fall der sogenannten zerlegbaren Formen, d. h. der homogenen Funktionen von beliebig hohem Grade n mit n Variabelen, welche rationale Koeffizienten haben und in n lineare Faktoren mit algebraischen Koeffizienten zerlegbar sind. Das Verdienst, diese Formen zuerst betrachtet und eine charakteristische Fundamental-Eigenschaft derselben erkannt zu haben, gebührt Lagrange**), und eine weitere Verfolgung seines Gedankens hätte leicht schon früher zu der Theorie der Komposition der Formen führen können. Erst viel später hat sich Dirichlet eingehend mit diesem Gegenstand beschäftigt; leider ist von seinen tiefen Untersuchungen — abgesehen von der ebenfalls hierhergehörigen, aber speziellen Theorie der quadratischen Formen mit komplexen Koeffizienten und Variabelen***) — nur eine einzige veröffentlicht, welche die Theorie der Transformation dieser Formen in sich selbst, oder, anders ausgedrückt, die Theorie der Einheiten in dem entsprechenden Gebiete algebraischer Zahlen behandelt. Der in äußerst kurzen Umrissen von Dirichlet mitgeteilte Beweis****) für die Existenz und für die allgemeine Form aller dieser Einheiten, welcher ihm erst nach großen und anhaltenden Anstrengungen gelungen ist, muß zu seinen bedeutendsten Leistungen gezählt werden, da derselbe ein unerläßliches Fundament für die ganze Theorie bildet; und Dirichlet selbst, der seinen eigenen Schöpfungen gegenüber sich immer ein ganz unbefangenes Urteil bewahrte, legte auf dies Resultat einen ebenso hohen Wert, wie auf die Prinzipien, welche ihn zu dem Beweise des Satzes über die arithmetische Progression und zur Bestimmung der Klassen-Anzahl der binären quadratischen Formen geführt haben. Dirichlet hat auch die Klassen-Anzahl für solche zerlegbare Formen bestimmt, welche aus der Theorie der

*) Ob dasselbe auch von der scharfsinnigen Methode gilt, welche R. Lipschitz zur Lösung derselben Aufgabe angewandt hat (Crelles Journal, Bd. 53), wage ich für jetzt nicht zu beurteilen; doch spricht dafür der Erfolg, mit welchem er diese Methode auf ein höheres Problem übertragen hat (Crelles Journal, Bd. 54).

**) Sur la solution des problèmes indéterminés du second degré. § VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. — Élémens d'Algèbre par L. Euler; Additions § IX.

***) Crelles Journal, Bd. 24.

****) Monatsberichte der Berliner Akademie vom Oktober 1841, April 1842, März 1846. — Comptes rendus der Pariser Akademie 1840, T. X, S. 286.

Kreisteilung entspringen, aber hiervon ist nichts veröffentlicht *). Es folgte zunächst im Jahre 1844 eine wertvolle Untersuchung von Eisenstein**) über gewisse kubische Formen, welche aus der Kreisteilung entspringen; doch scheint dieselbe wegen ihres sehr speziellen Charakters keinen bedeutenden Einfluß auf die Entwicklung der allgemeinen Theorie ausgeübt zu haben. Den größten und folgenreichsten Schritt aber hat Kummer***) im Jahre 1847 durch die Einführung der idealen Zahlen getan; denn wenn auch seine Untersuchungen ebenfalls sich zunächst nur auf die Kreisteilung und einige derselben nahestehende Gebiete beziehen, so sind doch die ihnen zugrunde liegenden Gedanken von viel allgemeinerer Bedeutung. Der außerordentliche, von Kummer erreichte Erfolg hat mich schon seit dem Jahre 1856 angetrieben, meine Kräfte hauptsächlich diesem Gegenstand zu widmen, und es ist mir endlich gelungen, eine allgemeine, ausnahmslose Theorie der ganzen algebraischen Zahlen aufzustellen, deren Grundlagen ich in dem zehnten Supplement der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie veröffentlicht habe****). Mit Hilfe dieser Prinzipien, welche ich hier als bekannt voraussetzen muß, läßt sich nun das auf die zerlegbaren Formen von beliebigem Grade oder auf die entsprechenden Ideal-Klassen übertragene Problem, das Verhältnis der Klassen-Anzahlen für verschiedene Ordnungen zu bestimmen, sowohl nach der Methode von Gauß, als auch nach derjenigen von Dirichlet vollständig lösen, und hierin besteht das Ziel der vorliegenden Abhandlung.

§ 1.

Theorie der ganzen Zahlen eines endlichen Körpers.

Obwohl diese Theorie, deren Mittelpunkt die Lehre von der Multiplikation der Ideale und von der Komposition der Ideal-Klassen bildet, hier als bekannt vorausgesetzt werden muß, so wird es doch

---

*) Vgl. Kummer, Gedächtnisrede auf G. P. Lejeune Dirichlet, 1860, S. 21—22.

**) Crelles Journal, Bd. 28.

***) Ebenda, Bd. 35.

****) Eine etwas ausführlichere Darstellung eines Teiles dieser Theorie erscheint gegenwärtig unter dem Titel *Sur la théorie des nombres entiers algébriques* in dem *Bulletin des sciences mathématiques et astronomiques* von Darboux und Houël. — Ich werde diese Abhandlung mit B. zitieren. [Vgl. Bd. 3 dieser Ausgabe.]

zweckmäßig sein, die wichtigsten ihr zugrunde liegenden Begriffe hier möglichst kurz in Erinnerung zu bringen, schon um den Anknüpfungspunkt der jetzigen Abhandlung an meine früheren Untersuchungen deutlicher hervorheben zu können.

Ist θ eine algebraische Zahl, und zwar eine Wurzel einer irreduktiblen Gleichung

$$f(\theta) = \theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

vom $n$ten Grade, deren Koeffizienten $a_1, a_2 \cdots a_{n-1}, a_n$ rationale Zahlen sind, und betrachtet man die sämtlichen Zahlen von der Form

$$\omega = \varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1},$$

wo $x_0, x_1, x_2 \cdots x_{n-1}$ willkürliche rationale Zahlen bedeuten, so besitzt der Inbegriff Ω aller dieser Zahlen ω die charakteristische Eigenschaft eines Körpers (D. § 159), welche darin besteht, daß die Summen, Differenzen, Produkte und Quotienten von je zwei solchen Zahlen ω ebenfalls in Ω enthalten sind; ein Körper Ω, dessen Zahlen auf die angegebene Art aus einer Wurzel θ einer irreduktiblen Gleichung $n$ten Grades gebildet sind, heißt speziell ein endlicher Körper vom Grade n. Hat man n Zahlen

$$\omega_1 = \varphi_1(\theta),\ \omega_2 = \varphi_2(\theta) \cdots \omega_n = \varphi_n(\theta)$$

nach Belieben, nur mit der einzigen Beschränkung aus Ω ausgewählt, daß die aus den n^2 rationalen Koeffizienten x gebildete Determinante einen von 0 verschiedenen Wert besitzt, so läßt sich jede beliebige Zahl ω des Körpers Ω stets und nur auf eine einzige Weise in der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

darstellen, wo $h_1, h_2 \cdots h_n$ rationale Zahlen bedeuten. Ein solches System von n Zahlen $\omega_1, \omega_2 \cdots \omega_n$ heißt eine Basis des Körpers Ω, und die n rationalen Zahlen $h_1, h_2 \cdots h_n$ heißen die Koordinaten der Zahl ω in bezug auf diese Basis. Offenbar bilden die Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ selbst eine solche Basis.

Ist θ' ebenfalls eine Wurzel derselben irreduktiblen Gleichung $f(\theta') = 0$, so entspricht jeder bestimmten Zahl $\omega = \varphi(\theta)$ des Körpers Ω eine bestimmte Zahl $\omega' = \varphi(\theta')$, und der Inbegriff aller dieser Zahlen ω' bildet einen mit Ω konjugierten Körper Ω'; diese Korrespondenz besitzt die charakteristische Eigenschaft, daß, wenn α, β zwei beliebige Zahlen des Körpers Ω bedeuten, stets

$$(\alpha+\beta)' = \alpha'+\beta',\ (\alpha-\beta)' = \alpha'-\beta',\ (\alpha\beta)' = \alpha'\beta',\ \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

ist; die Substitution, durch welche jede Zahl $\omega = \varphi(\theta)$ des Körpers Ω in die korrespondierende oder konjugierte Zahl $\omega' = \varphi(\theta')$ des Körpers Ω' übergeht, heiße eine Permutation des Körpers Ω. Sind $\theta', \theta'' \cdots \theta^{(n)}$ die sämtlichen Wurzeln der obigen irreduktiblen Gleichung, so entspricht einer jeden von ihnen, $\theta^{(r)}$, eine Permutation $P^{(r)}$ des Körpers Ω, durch welche jede in ihm enthaltene Zahl $\omega = \varphi(\theta)$ in die konjugierte Zahl $\omega^{(r)} = \varphi(\theta^{(r)})$ des Körpers $\Omega^{(r)}$ übergeht. Die n mit ω konjugierten Zahlen $\omega', \omega'' \cdots \omega^{(n)}$ sind dann immer die Wurzeln einer Gleichung $n$ten Grades mit rationalen Koeffizienten, welche aber nicht notwendig irreduktibel ist. Das Produkt $\omega'\omega'' \cdots \omega^{(n)}$ aus diesen n Zahlen ist eine rationale Zahl, welche die Norm der Zahl ω heißt und mit $N(\omega)$ bezeichnet wird; sie verschwindet nur dann, wenn $\omega = 0$ ist, und die Norm eines Produkts ist das Produkt aus den Normen der Faktoren. Sind ferner $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen des Körpers, so ist das Quadrat der Determinante

$$\sum \pm \alpha_1' \alpha_2'' \cdots \alpha_n^{(n)},$$

welche aus den n^2 konjugierten Zahlen $\alpha_i^{(k)}$ gebildet ist, ebenfalls eine rationale Zahl, welche die Diskriminante des Systems $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt und mit $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ bezeichnet wird; dieselbe ist stets und nur dann von 0 verschieden, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden; dies ergibt sich leicht aus dem bekannten Satze

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = (-1)^{1/2 n(n-1)} N[f'(\theta)],$$

wo $f'(t)$ die Derivierte der Funktion $f(t)$ bedeutet.

Alle algebraischen Zahlen, deren Gesamtheit ebenfalls einen Körper, aber keinen endlichen Körper bildet, zerfallen nun in ganze und in gebrochene Zahlen; eine algebraische Zahl η heißt eine ganze Zahl, wenn sie die Wurzel einer Gleichung von der Form

$$\eta^m + c_1 \eta^{m-1} + c_2 \eta^{m-2} + \cdots + c_{m-1}\eta + c_m = 0$$

ist, wo $c_1, c_2 \cdots c_{m-1}, c_m$ ganze Zahlen im alten Sinne des Wortes bedeuten, die von nun an immer rationale ganze Zahlen genannt werden sollen. Aus dieser Definition, welche wohl die höchste Verallgemeinerung des ursprünglich so beschränkten Begriffes der ganzen Zahl enthält, folgt unmittelbar, daß die Summen, Differenzen und Produkte von je zwei ganzen Zahlen wieder ganze Zahlen sind, und hieran knüpft sich wieder der Begriff der Teilbarkeit der ganzen Zahlen: eine ganze Zahl α heißt teilbar durch eine ganze Zahl β,

oder ein Vielfaches (Multiplum) von β, wenn $\alpha = \beta\gamma$, und γ wieder eine ganze Zahl ist; zugleich heißt γ ein Teiler (Divisor) von α, oder man sagt auch, β gehe in α auf. Eine ganze Zahl ε, welche in der Zahl 1 und folglich auch in allen ganzen Zahlen aufgeht, heißt eine Einheit; zwei ganze Zahlen, deren jede in der anderen aufgeht, und deren Quotient notwendig eine Einheit ist, heißen assoziierte Zahlen*) oder Gefährten.

Kehrt man mit diesen allgemeinen Begriffen zu einem endlichen Körper Ω zurück, und bezeichnet man mit $\mathfrak{o}$ den Inbegriff aller in Ω enthaltenen ganzen Zahlen, zu welchen auch alle ganzen rationalen Zahlen gehören, so ergibt sich ohne Schwierigkeit die Existenz einer aus n ganzen Zahlen $\omega_1, \omega_2 \cdots \omega_n$ bestehenden Basis des Körpers Ω von der Beschaffenheit, daß die Koordinaten $h_1, h_2 \cdots h_n$ einer jeden in $\mathfrak{o}$ enthaltenen Zahl

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

ganze rationale Zahlen sind; die Diskriminante

$$D = \Delta(\omega_1, \omega_2 \cdots \omega_n)$$

eines solchen Systems $\omega_1, \omega_2 \cdots \omega_n$, welches auch eine Basis des Gebietes $\mathfrak{o}$ heißen soll, ist eine ganze rationale, von 0 verschiedene Zahl, die ich ihrer Wichtigkeit wegen die Grundzahl oder die Diskriminante des Körpers Ω nenne und mit $\Delta(\Omega)$ bezeichne. Die Norm einer jeden von 0 verschiedenen Zahl μ des Gebietes $\mathfrak{o}$ ist eine ganze rationale, von 0 verschiedene Zahl, welche die folgende, wichtige Bedeutung besitzt; nennt man zwei ganze Zahlen α, β kongruent oder inkongruent in bezug auf den Modulus μ, je nachdem ihre Differenz $\alpha - \beta$ durch μ teilbar oder nicht teilbar ist, so ist die Anzahl aller in $\mathfrak{o}$ enthaltenen, nach μ inkongruenten Zahlen $= \pm N(\mu)$; die Kongruenz der Zahlen α, β in bezug auf μ wird durch $\alpha \equiv \beta \pmod{\mu}$ bezeichnet. Eine in $\mathfrak{o}$ enthaltene Einheit ist dadurch charakterisiert, daß ihre Norm $= \pm 1$ ist.

Die wichtigste Frage ist aber die nach der Zerlegung einer in $\mathfrak{o}$ enthaltenen Zahl μ in solche Faktoren, welche, wie im folgenden immer stillschweigend vorausgesetzt wird, ebenfalls dem Gebiet $\mathfrak{o}$ angehören. Die Divisoren einer Einheit sind sämtlich selbst Einheiten; ist aber μ keine Einheit, so sind zwei Fälle möglich; ist μ

*) Vgl. Gauß, Theoria residuorum biquadraticorum II, Art. 31.

das Produkt aus zwei Faktoren, von denen keiner eine Einheit, und folglich auch keiner mit μ assoziiert ist, so soll μ eine zerlegbare Zahl heißen; im entgegengesetzten Falle, d. h. wenn jeder Divisor von μ entweder ein Gefährte von μ oder eine Einheit ist, heißt μ unzerlegbar. Aus dem Satze über die Norm eines Produktes folgt nun offenbar, daß jede zerlegbare Zahl stets als Produkt aus einer endlichen Anzahl von unzerlegbaren Faktoren darstellbar ist; während aber in der Theorie der rationalen Zahlen (d. h. im Falle $n = 1$) diese Zerlegung, abgesehen von den Einheitsfaktoren ± 1, eine völlig bestimmte, einzige ist, so tritt bei Körpern höheren Grades sehr häufig die merkwürdige Erscheinung auf, daß eine Zahl μ als Produkt von unzerlegbaren Faktoren auf mehrere Arten darstellbar ist, welche in dem Sinne wesentlich verschieden sind, daß z. B. ein unzerlegbarer Faktor α der einen Darstellung $\mu = \alpha\beta\gamma\cdots$ mit keinem der unzerlegbaren Faktoren $\alpha_1, \beta_1\cdots$ der anderen Darstellung $\mu = \alpha_1\beta_1\cdots$ assoziiert ist. Es folgt hieraus, daß eine unzerlegbare Zahl durchaus nicht immer den Charakter einer eigentlichen Primzahl besitzt, welcher darin besteht, daß ein Produkt nur dann durch eine Primzahl teilbar ist, wenn diese wenigstens in einem der Faktoren aufgeht. Diese unwillkommene Erscheinung, welche auf den ersten Blick jeden weiteren Fortschritt auf diesem Felde zu verbieten schien, ist aber die Quelle von einer der schönsten und fruchtbarsten Entdeckungen in der höheren Arithmetik geworden: in der Tat ist Kummer bei der Untersuchung solcher Gebiete o, welche aus der Kreisteilung entspringen, dahin gelangt, die Gesetze der Teilbarkeit durch Einführung idealer Zahlen in völligen Einklang mit denjenigen zu bringen, welche in der alten Theorie der rationalen Zahlen herrschen.

Es ist das Ziel meiner langjährigen Bemühungen gewesen, dasselbe Resultat für jeden endlichen Körper Ω zu erreichen, also diejenigen allgemeinen Gesetze der Teilbarkeit festzustellen, welche ohne Ausnahme jedem Gebiete o von der oben beschriebenen Art zukommen. Bei der Begründung dieser Theorie (D. § 163) habe ich den von Kummer eingeschlagenen Weg verlassen und statt der idealen Zahlen einen anderen Begriff, den des Ideals, einführen müssen, welcher von jeder, einem speziellen Körper Ω eigentümlichen Färbung frei ist und gerade deshalb die erforderliche Allgemeinheit besitzt, um als Grundlage der Theorie dienen zu können. Zum Ver-

ständnis der nachfolgenden Untersuchungen ist es unerläßlich, an die Hauptsätze dieser Theorie kurz zu erinnern.

1°. Ein System $\mathfrak{m}$ von unendlich vielen Zahlen des Gebietes $\mathfrak{o}$ heißt ein Ideal, wenn es die beiden folgenden Eigenschaften besitzt:

I. Die Summen und Differenzen von je zwei Zahlen des Systems $\mathfrak{m}$ sind ebenfalls in $\mathfrak{m}$ enthalten.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{m}$ und aus einer Zahl des Systems $\mathfrak{o}$ ist eine Zahl des Systems $\mathfrak{m}$.

Bedeutet μ eine bestimmte, ω jede beliebige Zahl in $\mathfrak{o}$, so kommen diese beiden Eigenschaften offenbar dem System $\mathfrak{m}$ aller durch μ teilbaren Zahlen $\mu\omega$ zu; ein solches Ideal $\mathfrak{m}$ heißt ein Hauptideal und wird mit $\mathfrak{o}(\mu)$ oder kürzer mit $\mathfrak{o}\mu$ oder $\mu\mathfrak{o}$ bezeichnet*); es bleibt ungeändert, wenn μ durch eine mit μ assoziierte Zahl ersetzt wird. Ist μ eine Einheit, so ist $\mathfrak{o}\mu = \mathfrak{o}$, und umgekehrt. Da die Kongruenz zweier Zahlen α, β in bezug auf den Modulus μ darin besteht, daß die Differenz $\alpha - \beta$ dem Ideal $\mathfrak{o}\mu$ angehört, so wird man zu der folgenden allgemeineren Definition der Kongruenz geführt:

2°. Zwei Zahlen α, β heißen kongruent in bezug auf ein Ideal $\mathfrak{m}$, und dies wird durch die Kongruenz $\alpha \equiv \beta \pmod{\mathfrak{m}}$ angedeutet, wenn $\alpha - \beta$ eine Zahl des Ideals $\mathfrak{m}$ ist; im entgegengesetzten Falle heißen α, β inkongruent nach $\mathfrak{m}$. Die immer endliche Anzahl aller in $\mathfrak{o}$ enthaltenen, in bezug auf $\mathfrak{m}$ inkongruenten Zahlen heißt die Norm des Ideals $\mathfrak{m}$ und wird mit $N(\mathfrak{m})$ bezeichnet; die Norm eines Hauptideals $\mathfrak{o}\mu$ ist $= \pm N(\mu)$; das Hauptideal $\mathfrak{o}$ ist das einzige Ideal, dessen Norm $= 1$ ist.

Die Teilbarkeit einer Zahl $\mu = \alpha\beta$ durch eine Zahl α besteht darin, daß alle Zahlen $\mu\omega = \alpha(\beta\omega)$ des Ideals $\mathfrak{o}\mu$ auch in dem Ideal $\mathfrak{o}\alpha$ enthalten sind; dies veranlaßt zu der folgenden Definition der Teilbarkeit der Ideale:

3°. Ein Ideal $\mathfrak{m}$ heißt teilbar durch ein Ideal $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Ideals $\mathfrak{m}$ auch dem Ideal $\mathfrak{a}$ angehören; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, oder man sagt auch, $\mathfrak{a}$ gehe in $\mathfrak{m}$ auf.

*) Früher habe ich die weniger zweckmäßige Bezeichnung $\mathfrak{i}(\mu)$ angewendet (D. § 163).

Da hiernach die Teilbarkeit der Zahlen nur einen speziellen Fall von der Teilbarkeit der Ideale bildet, so kommt es lediglich darauf an, die tatsächlich einfacheren Gesetze der letzteren festzustellen. Dies geschieht durch die folgenden Begriffe und Sätze:

4°. Ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, und letzteres teilbar durch das Ideal $\mathfrak{b}$, so ist auch $\mathfrak{m}$ teilbar durch $\mathfrak{b}$.

5°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so bildet das System $\mathfrak{m}$ aller den Idealen $\mathfrak{a}$, $\mathfrak{b}$ gemeinschaftlich angehörenden Zahlen ein Ideal, welches das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil es in jedem gemeinschaftlichen Vielfachen von $\mathfrak{a}$, $\mathfrak{b}$ aufgeht.

6°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bildet das System $\mathfrak{d}$ aller in der Form $\alpha + \beta$ darstellbaren Zahlen ein Ideal, welches der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideal $\mathfrak{d}$ aufgeht.

7°. Zwei Ideale, deren größter gemeinschaftlicher Teiler das Ideal $\mathfrak{o}$ ist, heißen relative Primideale.

8°. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heißt ein Primideal, wenn es kein von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenes Ideal zum Teiler hat; im entgegengesetzten Falle heißt $\mathfrak{p}$ ein zusammengesetztes Ideal.

9°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bilden die sämtlichen Produkte $\alpha\beta$ und alle Summen von solchen Produkten ein durch $\mathfrak{a}$ und durch $\mathfrak{b}$ teilbares Ideal, welches das Produkt aus den Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ heißt und mit $\mathfrak{ab} = \mathfrak{ba}$ bezeichnet wird; zugleich ist $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Die Ausdehnung dieses Begriffes auf beliebig viele Faktoren und die Bedeutung einer Potenz ist selbstverständlich.

10°. Umgekehrt: ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$ von der Art, daß $\mathfrak{ab} = \mathfrak{m}$ wird.

11°. Ein Produkt von Idealen ist nur dann durch ein Primideal teilbar, wenn dieses wenigstens in einem der Faktoren aufgeht.

12°. Jedes zusammengesetzte Ideal ist als Produkt von lauter Primidealen darstellbar, und zwar nur auf eine einzige Weise.

13°. Damit ein Ideal $\mathfrak{m}$ durch ein Ideal $\mathfrak{a}$ teilbar sei, ist erforderlich und hinreichend, daß alle in $\mathfrak{a}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen.

14°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so gibt es ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{a}\mathfrak{m}$ von der Art, daß $\mathfrak{m}$ und $\mathfrak{b}$ relative Primideale werden.

Für den Fall $n = 1$, in welchem alle Ideale Hauptideale sind, gehen die vorstehenden Sätze, deren strenge Beweise mir erst nach Überwindung von erheblichen Schwierigkeiten gelungen sind, in die Fundamentalsätze über die Teilbarkeit der ganzen rationalen Zahlen über. Dieselben Gesetze gelten daher auch für jeden Körper Ω von beliebigem Grade n, sobald alle seine Ideale Hauptideale sind, und für einen solchen Körper ist offenbar die Einführung der Ideale gänzlich überflüssig. Dies ist aber, wie schon oben bemerkt, im allgemeinen keineswegs der Fall, und hieran knüpft sich die Einteilung aller Ideale eines Körpers Ω in bestimmte Ideal-Klassen (D. § 164). Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen äquivalent, wenn es ein Ideal $\mathfrak{c}$ gibt, für welches beide Produkte $\mathfrak{a}\mathfrak{c}$, $\mathfrak{b}\mathfrak{c}$ Hauptideale werden; da aus dieser Definition unmittelbar folgt, daß zwei mit einem dritten äquivalente Ideale auch miteinander äquivalent sind, so bildet das System A aller Ideale, welche einem bestimmten Ideal $\mathfrak{a}$ äquivalent sind, eine Klasse, welche ungeändert bleibt, wenn ihr Repräsentant $\mathfrak{a}$ durch ein beliebiges, derselben Klasse A angehörendes Ideal ersetzt wird. Die Anzahl h dieser Klassen ist immer eine endliche; wählt man aus jeder Klasse nach Belieben ein bestimmtes Ideal als Repräsentanten, so ist jedes Ideal mit einem und nur mit einem dieser h Ideale äquivalent. Das System aller Hauptideale bildet die Hauptklasse O; zu jeder Klasse A von Idealen $\mathfrak{a}$ gehört eine bestimmte entgegengesetzte oder reziproke, inverse Klasse A^{-1}, welche aus allen denjenigen Idealen besteht, die durch Multiplikation mit den Idealen $\mathfrak{a}$ in Hauptideale verwandelt werden. Durchläuft nun $\mathfrak{a}$ alle Ideale einer Klasse A, ebenso $\mathfrak{b}$ alle Ideale einer Klasse B, so gehören die sämtlichen Produkte $\mathfrak{a}\mathfrak{b}$ ein und derselben Klasse an, welche die aus A und B zusammengesetzte Klasse oder das Produkt aus A, B heißt und mit AB bezeichnet wird; diese Komposition oder Multiplikation der Ideal-Klassen gehorcht den Gesetzen $AB = BA$, $(AB)C = A(BC)$, $OA = A$, $AA^{-1} = O$, $A^r A^s = A^{r+s}$, $A^h = O$, und aus $AB = AC$ folgt $B = C$.

Aus dem Satze $A^h = O$ folgt beiläufig, wenn man von dem endlichen Körper Ω wieder zu dem Gebiete aller ganzen algebraischen Zahlen übergeht, das wichtige Resultat, daß je zwei ganze Zahlen

α, β, die nicht beide verschwinden, einen größten gemeinschaftlichen Divisor δ besitzen, welcher in der Form $\delta = \alpha\alpha_1 + \beta\beta_1$ darstellbar ist, wo α_1, β_1 ebenfalls ganze Zahlen bedeuten; natürlich kann auch hier δ durch jeden Gefährten von δ ersetzt werden.

Das größte Interesse nimmt aber die Bestimmung der Klassen-Anzahl h in Anspruch (D. § 167). Die Übertragung der Prinzipien, welche Dirichlet bei dem Beweise des Satzes über die arithmetische Progression und bei der Bestimmung der Klassen-Anzahl der binären quadratischen Formen geschaffen hat, führt zu der Betrachtung unendlicher Reihen und Produkte von der Form

$$\sum f(\mathfrak{a}) = \prod \frac{1}{1 - f(\mathfrak{p})},$$

wo $\mathfrak{a}$ alle Ideale, $\mathfrak{p}$ alle Primideale durchläuft, und $f(\mathfrak{a})$ eine reelle oder komplexe Funktion bedeutet, die der Bedingung $f(\mathfrak{ab}) = f(\mathfrak{a})f(\mathfrak{b})$ genügt und außerdem so beschaffen ist, daß die unendliche Reihe linker Hand eine von der Anordnung ihrer Glieder unabhängige endliche Summe besitzt. Diese Bedingungen sind erfüllt, wenn man

$$f(\mathfrak{a}) = \frac{1}{N(\mathfrak{a})^s}, \quad s > 1$$

nimmt; multipliziert man mit $(s-1)$ und teilt die Totalsumme in h Partialsummen, deren jede einer bestimmten Klasse von Idealen $\mathfrak{a}$ entspricht, so nähern sich diese Summen für unendlich kleine positive Werte von $(s-1)$ einem gemeinschaftlichen, endlichen, von 0 verschiedenen Grenzwert g, der sich nach den fundamentalen Untersuchungen Dirichlets über die Einheiten ohne Schwierigkeit bestimmen läßt, und man erhält folglich

$$gh = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = \lim (s-1) \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}.$$

Das Problem der Klassen-Anzahl wird daher gelöst sein, sobald es gelingt, den Grenzwert der unendlichen Reihe oder des mit ihr identischen Produkts noch auf eine zweite Art, nämlich unmittelbar aus der Natur der sämtlichen, dem Körper Ω angehörenden Primideale $\mathfrak{p}$ zu bestimmen. Dies ist bis jetzt nur für Kreisteilungskörper geglückt (zu welchen auch alle quadratischen Körper gehören), und eine aufmerksame Betrachtung dieser Fälle führt zu der

Überzeugung — in welcher ich durch meine demnächst zu veröffentlichenden Untersuchungen über die Anzahl der Ideal-Klassen in kubischen Körpern bestärkt werde —, daß die allgemeine Lösung des Problems der Klassen-Anzahl auf diesem Wege erst dann gelingen wird, wenn die algebraische Konstitution eines jeden Körpers und ihr Zusammenhang mit seinen Idealen uns vollständig bekannt sein wird — ein Ziel, von welchem wir noch außerordentlich weit entfernt sind; außerdem scheint auch eine viel genauere Ausbildung der Theorie der transzendenten Funktionen erforderlich zu sein.

Es ist nun noch mit einigen Worten die Beziehung zwischen den Idealen eines Körpers und den zugehörigen zerlegbaren Formen zu besprechen (D. § 165). Ist $\mathfrak{a}$ ein bestimmtes Ideal, so gibt es immer n partikuläre, in $\mathfrak{a}$ enthaltene Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ von der Beschaffenheit, daß die sämtlichen Zahlen α des Ideals $\mathfrak{a}$ durch den Ausdruck

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

dargestellt werden, wenn die Variabelen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen. Das System der Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt eine Basis von $\mathfrak{a}$. Bildet man das Produkt aus allen n mit α konjugierten Ausdrücken, so erhält man

$$N(\alpha) = N(\mathfrak{a})X,$$

wo X eine homogene Funktion $n$ten Grades von den Variabelen $x_1, x_2 \cdots x_n$ bedeutet; die Koeffizienten dieser zerlegbaren Form X sind immer ganze rationale Zahlen ohne gemeinschaftlichen Teiler. Da das Ideal $\mathfrak{a}$ unendlich viele verschiedene Basen besitzt, so entspricht demselben eine Klasse von unendlich vielen äquivalenten Formen X, welche durch lineare Substitutionen mit ganzen rationalen Koeffizienten gegenseitig ineinander übergehen. Dieselben Formen entspringen aber auch aus jedem mit $\mathfrak{a}$ äquivalenten Ideal, und folglich entspricht jeder Ideal-Klasse eine bestimmte Formen-Klasse. Die Multiplikation der Ideale und der Ideal-Klassen führt zu der Komposition der Formen und der Formen-Klassen.

Aber diese Formen X umfassen nur einen unendlich kleinen Teil aller möglichen zu dem Körper Ω gehörenden Formen. Versteht man nämlich unter der Determinante einer aus n homogenen linearen Faktoren $f_1, f_2 \cdots f_n$ gebildeten Funktion F von

n Variabelen $h_1, h_2 \cdots h_n$ das Quadrat der Funktional-Determinante

$$\sum \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n},$$

so ergibt sich leicht, daß die Determinante aller oben betrachteten Formen X mit der Grundzahl $D = \Delta(\Omega)$ des Körpers Ω übereinstimmt; für den Fall $n = 2$ würde man z. B. nur zu solchen binären Formen $ax^2 + bxy + cy^2$ gelangen, deren Determinante $b^2 - 4ac = D$ durch kein ungerades Quadrat teilbar und entweder $\equiv 1 \pmod 4$, oder $\equiv 8, 12 \pmod{16}$ ist*).

Um nun eine allgemeinere Theorie der zu einem Körper Ω gehörenden Formen aufzustellen, muß man, wie ich schon früher bemerkt habe (D. § 165), den Begriff des Ideals so erweitern, daß an Stelle des bisher betrachteten Gebietes $\mathfrak{o}$, welches alle ganzen Zahlen des Körpers umfaßt, beschränktere Gebiete $\mathfrak{o}'$ treten, welche ich mit Rücksicht auf die in der Theorie der binären quadratischen Formen von Gauß gebrauchte Ausdrucksweise Ordnungen genannt habe. Diese Erweiterung bildet den nächsten Gegenstand dieser Abhandlung.

§ 2.

Sätze aus der Theorie der Moduln.

Um hierzu zu gelangen, und namentlich um beständige Wiederholungen über die Art zu vermeiden, in welcher aus gewissen Systemen von Zahlen neue Systeme gebildet werden, ist es notwendig, hier einige sehr einfache und zugleich sehr allgemeine Sätze über solche Systeme einzuschalten, die ich Moduln genannt habe (D. § 161). Da der Begriff eines Ideals in demjenigen eines Moduls als spezieller Fall enthalten ist, so wird bei einer systematischen Darstellung die Theorie der Moduln zweckmäßig der Theorie der Ideale vorausgeschickt werden. Hier wird es genügen, einige Hauptbegriffe zu entwickeln und einige Sätze anzuführen, deren Beweise ich unterdrücke, weil jeder sie leicht finden wird (vgl. D. § 161 und B. §§ 1

*) Die obige Erklärung einer Formen-Determinante stimmt für den Fall $n = 2$ nicht ganz mit derjenigen von Gauß überein; dies läßt sich aber kaum vermeiden, wenn sie allgemein für jeden Grad n gelten soll, und selbst in dem speziellen Falle $n = 2$ sprechen viele Erscheinungen zugunsten derselben, was ich aber hier nicht näher begründen kann.

bis 4). Da manche dieser Sätze sich in Worten nur ziemlich umständlich aussprechen lassen, so wage ich es, die Ausdrucksweise durch Einführung einer Zeichensprache abzukürzen, und ich hoffe, daß man aus diesem Grunde die Benutzung der Zeichen $>$, $<$, $+$, $-$ entschuldigen wird. Ich bemerke nur noch, daß im folgenden die Einschränkung auf die Zahlen eines endlichen Körpers gänzlich wegfällt, also das Wort Zahl immer in seiner allgemeinsten Bedeutung gebraucht wird.

1°. Ein System $\mathfrak{m}$ von reellen oder komplexen Zahlen heißt ein Modul, wenn alle Summen und Differenzen dieser Zahlen demselben System $\mathfrak{m}$ angehören. Die Zahl 0 findet sich in jedem Modul, und sie bildet auch für sich allein einen Modul. Ein Modul $\mathfrak{m}$ heißt teilbar durch einen Modul $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Moduls $\mathfrak{m}$ auch in $\mathfrak{a}$ enthalten sind; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, und wir bezeichnen die Teilbarkeit von $\mathfrak{m}$ durch $\mathfrak{a}$ sowohl durch $\mathfrak{m} > \mathfrak{a}$, als durch $\mathfrak{a} < \mathfrak{m}$. Ist jeder der beiden Moduln $\mathfrak{m}$, $\mathfrak{a}$ durch den anderen teilbar, so sind sie identisch, was durch $\mathfrak{m} = \mathfrak{a}$ angedeutet wird. Aus $\mathfrak{m} > \mathfrak{a}$, $\mathfrak{a} > \mathfrak{b}$ folgt $\mathfrak{m} > \mathfrak{b}$. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so ist das System aller derjenigen Zahlen, welche beiden Moduln gemeinschaftlich angehören, selbst ein Modul, und zwar ein Vielfaches von $\mathfrak{a}$ und von $\mathfrak{b}$, welches durch $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnet werden soll; dasselbe heißt das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{a} - \mathfrak{b}$ teilbar ist. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so ist das System aller Zahlen von der Form $\alpha + \beta$ ein Modul, und zwar ein Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$, der mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ bezeichnet werden soll; derselbe heißt der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ auch ein Teiler von $\mathfrak{a} + \mathfrak{b}$ ist. Diese Begriffe lassen sich leicht auf beliebig viele, sogar auf unendlich viele Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \cdots$ ausdehnen, und man beweist leicht die beiden folgenden charakteristischen Sätze

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c})),$$
$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c})),$$

in welchen sich der zwischen den Begriffen des kleinsten gemeinschaftlichen Vielfachen und des größten gemeinschaftlichen Teilers durchgängig herrschende Dualismus kundgibt.

2°. Zwei Zahlen α, β heißen kongruent oder inkongruent in bezug auf einen Modul $\mathfrak{m}$, je nachdem ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten ist oder nicht; die Kongruenz wird durch $\alpha \equiv \beta \pmod{\mathfrak{m}}$ ausgedrückt. Alle mit einer bestimmten Zahl nach $\mathfrak{m}$ kongruenten Zahlen bilden eine Zahl-Klasse (mod. $\mathfrak{m}$). Mehrere Zahlen heißen inkongruent (mod. $\mathfrak{m}$), wenn jede derselben mit jeder der übrigen inkongruent (mod. $\mathfrak{m}$) ist. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so kann es sein, daß $\mathfrak{a}$ nur eine endliche Anzahl inkongruenter Zahlen in bezug auf $\mathfrak{b}$ enthält, und dann soll diese Anzahl durch das Symbol $(\mathfrak{a}, \mathfrak{b})$ bezeichnet werden; gibt es aber in $\mathfrak{a}$ unendlich viele, in bezug auf $\mathfrak{b}$ inkongruente Zahlen, so soll $(\mathfrak{a}, \mathfrak{b}) = 0$ gesetzt werden, weil dann gewisse Determinanten-Sätze allgemein gültig bleiben. In beiden Fällen ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b});$$

ist $\mathfrak{a} > \mathfrak{b}$, so ist $(\mathfrak{a}, \mathfrak{b}) = 1$, und umgekehrt. Ist ferner $\mathfrak{m} > \mathfrak{a} > \mathfrak{b}$, so ist

$$(\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})(\mathfrak{a}, \mathfrak{m}).$$

Durch Kombination beider Sätze erhält man viele andere Sätze, die hier übergangen werden können. Sind ϱ, σ zwei gegebene Zahlen, so hat das System der beiden Kongruenzen

$$\omega \equiv \varrho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

stets und nur dann gemeinschaftliche Wurzeln ω, wenn

$$\varrho \equiv \sigma \pmod{\mathfrak{a} + \mathfrak{b}}$$

ist, und die sämtlichen Zahlen ω bilden eine bestimmte Zahlklasse (mod. $\mathfrak{a} - \mathfrak{b}$).

3°. Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ Konstanten, während $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, so bilden die sämtlichen, in der Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

darstellbaren Zahlen α einen Modul $\mathfrak{a}$, der ein endlicher Modul heißen und mit $[\alpha_1, \alpha_2 \cdots \alpha_n]$ bezeichnet werden soll; die Konstanten $\alpha_1, \alpha_2 \cdots \alpha_n$ bilden eine Basis des Moduls $\mathfrak{a}$. Der Modul [1] ist das System aller ganzen rationalen Zahlen. Wenn alle Zahlen eines solchen endlichen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ durch Multiplikation mit rationalen, von 0 verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{b}$ verwandelt werden können, so ist $(\mathfrak{a}, \mathfrak{b})$ von 0 verschieden, und $\mathfrak{a} - \mathfrak{b}$

ist ein endlicher Modul; man kann die ganzen rationalen Zahlen a so wählen, daß die n Zahlen

$$\begin{aligned}
\mu_1 &= a_1' \alpha_1, \\
\mu_2 &= a_1'' \alpha_1 + a_2'' \alpha_2, \\
\mu_3 &= a_1''' \alpha_1 + a_2''' \alpha_2 + a_3''' \alpha_3, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)} \alpha_1 + a_2^{(n)} \alpha_2 + a_3^{(n)} \alpha_3 + \cdots + a_n^{(n)} \alpha_n
\end{aligned}$$

eine Basis von $\mathfrak{a} - \mathfrak{b}$ bilden, und daß zugleich

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = a_1' a_2'' a_3''' \cdots a_n^{(n)}$$

wird; unterwirft man die n ganzen rationalen Zahlen $x_1', x_2' \cdots x_n'$ den n Bedingungen

$$0 \leqq x_r' < a_r^{(r)},$$

so sind die entsprechenden, in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha' = x_1' \alpha_1 + x_2' \alpha_2 + \cdots + x_n' \alpha_n,$$

deren Anzahl $= (\mathfrak{a}, \mathfrak{b})$ ist, sämtlich inkongruent (mod. $\mathfrak{b}$) und deshalb auch inkongruent (mod. $\mathfrak{a} - \mathfrak{b}$).

4°. Ein System von n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ soll ein irreduktibeles System, und diese Zahlen sollen voneinander unabhängig heißen, wenn die Summe

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

für jedes System von rationalen, nicht sämtlich verschwindenden Zahlen $x_1, x_2 \cdots x_n$ einen von 0 verschiedenen Wert erhält. Ist nun wieder $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$, und sind die Basiszahlen eines Moduls $\mathfrak{m} = [\mu_1, \mu_2 \cdots \mu_n]$ von der Form

$$\begin{aligned}
\mu_1 &= a_1' \alpha_1 + a_2' \alpha_2 + \cdots + a_n' \alpha_n, \\
\mu_2 &= a_1'' \alpha_1 + a_2'' \alpha_2 + \cdots + a_n'' \alpha_n, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)} \alpha_1 + a_2^{(n)} \alpha_2 + \cdots + a_n^{(n)} \alpha_n,
\end{aligned}$$

wo die Koeffizienten a ganze rationale Zahlen bedeuten, so ist

$$(\mathfrak{a}, \mathfrak{m}) = \pm \sum \pm a_1' a_2'' \cdots a_n^{(n)}.$$

Von besonderer Wichtigkeit ist noch der folgende Satz: besteht eine Basis eines endlichen Moduls $\mathfrak{a}$ aus m Zahlen $\alpha_1', \alpha_2' \cdots \alpha_m'$, von denen aber nur n voneinander unabhängig sind, so gibt es immer eine aus n unabhängigen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ bestehende Basis desselben Moduls $\mathfrak{a}$.

5°. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so bilden die Produkte $\alpha\beta$ und alle Summen solcher Produkte einen Modul, der das Produkt aus den Faktoren $\mathfrak{a}$, $\mathfrak{b}$ heißen und mit $\mathfrak{ab}$ bezeichnet werden soll, aber keineswegs durch $\mathfrak{a}$ oder $\mathfrak{b}$ teilbar zu sein braucht. Offenbar ist $\mathfrak{ab} = \mathfrak{ba}$ und $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc}) = \mathfrak{abc}$; die Bedeutung einer Potenz $\mathfrak{a}^r$ ist selbstverständlich. Aus $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{b}' > \mathfrak{b}$ folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{ab}$; ferner ist

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{ac} + \mathfrak{bc},$$
$$(\mathfrak{a} - \mathfrak{b})\mathfrak{c} > \mathfrak{ac} - \mathfrak{bc},$$
$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} - \mathfrak{b}) > \mathfrak{ab};$$

ist ferner $[1] > \mathfrak{o}$, so ist $\mathfrak{a} > \mathfrak{oa}$, weil $\mathfrak{a}[1] = \mathfrak{a}$ ist. Ist $\mathfrak{b}$ ein eingliedriger Modul $[\mu]$, so besteht das Produkt $\mathfrak{ab}$ aus den Produkten $\alpha\mu$, wo α alle Zahlen des Moduls $\mathfrak{a}$ durchläuft; ein solches Produkt $\mathfrak{a}[\mu]$ soll bequemer durch $\mathfrak{a}\mu = \mu\mathfrak{a}$ bezeichnet werden; dann ist $(\mathfrak{a}\mu)\nu = \mathfrak{a}(\mu\nu)$, und aus $\mathfrak{a}\mu = \mathfrak{a}'\mu$ folgt immer $\mathfrak{a} = \mathfrak{a}'$, wenn μ von 0 verschieden ist.

6°. Ist $\mathfrak{a}$ ein beliebiger Modul, so bildet das System $\mathfrak{o}$ aller derjenigen Zahlen ω, für welche das Produkt $\mathfrak{a}\omega > \mathfrak{a}$ wird, einen Modul, welcher die Ordnung des Moduls $\mathfrak{a}$ heißen soll und offenbar stets ein Teiler des Moduls $[1]$ ist; hieraus folgt unmittelbar, daß $\mathfrak{ao} = \mathfrak{a}$, und $\mathfrak{o}^2 = \mathfrak{o}$ ist. Umgekehrt ist jeder Modul $\mathfrak{o}$, der ein Teiler von $[1]$ und von $\mathfrak{o}^2$ ist, eine Ordnung, nämlich diejenige des Moduls $\mathfrak{o}$ selbst. Der Begriff einer Ordnung bildet eigentlich nur einen speziellen Fall des Begriffes des Quotienten $\mathfrak{a} : \mathfrak{b}$ von zwei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, worunter der größte gemeinschaftliche Teiler aller derjenigen Moduln $\mathfrak{c}$ zu verstehen ist, für welche das Produkt $\mathfrak{bc}$ durch $\mathfrak{a}$ teilbar wird; die Ordnung $\mathfrak{o}$ eines Moduls $\mathfrak{a}$ ist nämlich identisch mit dem Quotienten $\mathfrak{a} : \mathfrak{a}$, und die charakteristische Eigenschaft einer jeden Ordnung $\mathfrak{o}$ wird durch die Gleichung $\mathfrak{o} : \mathfrak{o} = \mathfrak{o}$ ausgedrückt. Doch wird von dem Begriff des Quotienten in dieser Abhandlung kein Gebrauch gemacht werden.

§ 3.

Ordnungen in einem endlichen Körper.

Nach diesen allgemeinen Vorbereitungen kehren wir definitiv zu den Zahlen eines endlichen Körpers Ω vom Grade n zurück, und beschränken zunächst den Begriff des Moduls in der Weise, daß unter einem Modul $\mathfrak{a}$ stets ein endlicher Modul $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verstanden

wird, dessen Basiszahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ zugleich eine Basis des Körpers Ω bilden (§ 1) und folglich voneinander unabhängig sind (§ 2, 4°). Da hiernach jede Zahl des Körpers Ω durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so ergibt sich aus den vorhergehenden allgemeinen Sätzen sehr leicht, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler, und ebenso das Produkt (und auch der Quotient) von je zwei solchen Moduln $\mathfrak{a}$, $\mathfrak{b}$ stets wieder ein solcher Modul, und daß $(\mathfrak{a}, \mathfrak{b})$ stets von 0 verschieden ist. Versteht man ferner wie früher, und wie es auch in der Folge stets geschehen soll, unter $\mathfrak{o}$ das Gebiet aller ganzen Zahlen des Körpers Ω, so kommt die Definition eines Ideals $\mathfrak{m}$ (§ 1, 1°) darauf hinaus, daß $\mathfrak{m}$ ein durch $\mathfrak{o}$ teilbarer Modul ist (I), welcher der Bedingung $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$ genügt (II); die dortigen Sätze 5°, 6°, 9° enthalten nur noch die Behauptung, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler und das Produkt von zwei beliebigen Idealen wieder Ideale sind; die Norm eines Ideals $\mathfrak{m}$ ist $= (\mathfrak{o}, \mathfrak{m})$.

Für die in Aussicht genommene Erweiterung des Ideal-Begriffs ist nun vor allem die Konstitution der Ordnung $\mathfrak{o}'$ eines beliebigen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ von Wichtigkeit (§ 2, 6°). Damit eine Zahl ω' der Ordnung $\mathfrak{o}'$ des Moduls $\mathfrak{a}$ angehöre, ist offenbar erforderlich und hinreichend, daß die n Produkte $\omega'\alpha_1, \omega'\alpha_2 \cdots \omega'\alpha_n$ in $\mathfrak{a}$ enthalten sind, daß also

$$\begin{aligned}
\omega'\alpha_1 &= x_1'\alpha_1 + x_2'\alpha_2 + \cdots + x_n'\alpha_n,\\
\omega'\alpha_2 &= x_1''\alpha_1 + x_2''\alpha_2 + \cdots + x_n''\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\\
\omega'\alpha_n &= x_1^{(n)}\alpha_1 + x_2^{(n)}\alpha_2 + \cdots + x_n^{(n)}\alpha_n
\end{aligned}$$

ist, wo die n^2 Koeffizienten x sämtlich ganze rationale Zahlen bedeuten. Aus jeder einzelnen dieser Gleichungen folgt zunächst, daß ω' eine Zahl des Körpers Ω ist, und wenn man die n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eliminiert, so erhält man

$$\begin{vmatrix}
x_1' - \omega', & x_2' & \cdots & x_n'\\
x_1'' & x_2'' - \omega' & \cdots & x_n''\\
\cdots & \cdots & \cdots & \cdots\\
x_1^{(n)} & x_2^{(n)} & \cdots & x_n^{(n)} - \omega'
\end{vmatrix} = 0,$$

d. h. ω' ist eine ganze algebraische Zahl, also in dem Gebiete $\mathfrak{o}$ enthalten; mithin ist $\mathfrak{o}'$ ein Vielfaches von $\mathfrak{o}$. Versteht man jetzt für

einen Augenblick unter ω' eine beliebige Zahl des Körpers Ω, so gehören auch die n Produkte $\omega'\alpha_1$, $\omega'\alpha_2 \cdots \omega'\alpha_n$ dem Körper Ω an, und folglich werden, da $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden, wieder n Gleichungen von der obigen Form stattfinden, in welchen aber die n^2 rationalen Koeffizienten x nicht mehr notwendig ganze Zahlen sind; es wird dann immer eine von 0 verschiedene, rationale Zahl m von der Art geben, daß die sämtlichen n^2 Produkte mx ganze Zahlen werden, und folglich wird das Produkt $m\omega'$ eine Zahl der Ordnung $\mathfrak{o}'$ sein; jede Zahl des Körpers Ω, also auch jede Zahl des Gebietes $\mathfrak{o}$ kann daher durch Multiplikation mit einer von 0 verschiedenen rationalen Zahl in eine Zahl der Ordnung $\mathfrak{o}'$ verwandelt werden, und da das Gebiet $\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n]$ ein Teiler von $\mathfrak{o}'$ ist, so ist (nach § 2, 3°) $\mathfrak{o}'$ ein endlicher Modul $[\omega_1', \omega_2' \cdots \omega_n']$, dessen Basiszahlen mit denen von $\mathfrak{o}$ durch n Gleichungen von der Form

$$\begin{aligned}
\omega_1' &= k_1'\omega_1 + k_2'\omega_2 + \cdots + k_n'\omega_n,\\
\omega_2' &= k_1''\omega_1 + k_2''\omega_2 + \cdots + k_n''\omega_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\omega_n' &= k_1^{(n)}\omega_1 + k_2^{(n)}\omega_2 + \cdots + k_n^{(n)}\omega_n
\end{aligned}$$

verbunden sind, deren Koeffizienten ganze rationale Zahlen sind und eine von 0 verschiedene, positive Determinante

$$\sum \pm k_1' k_2'' \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k$$

besitzen. Die charakteristischen Eigenschaften einer solchen Ordnung $\mathfrak{o}'$ sind daher (§ 2, 6°) die folgenden:

1°. $\mathfrak{o}'$ ist ein durch $\mathfrak{o}$ teilbarer Modul im obigen beschränkten Sinne des Wortes; alle in $\mathfrak{o}'$ enthaltenen Zahlen sind ganze Zahlen des Körpers Ω.

2°. $\mathfrak{o}'$ ist ein Teiler von [1], d. h. alle ganzen rationalen Zahlen sind in $\mathfrak{o}'$ enthalten.

3°. $\mathfrak{o}'$ ist ein Teiler von $\mathfrak{o}'^2$, d. h. jedes Produkt von zwei in $\mathfrak{o}'$ enthaltenen Zahlen gehört ebenfalls dem System $\mathfrak{o}'$ an. Aus 2° folgt dann $\mathfrak{o}'^2 = \mathfrak{o}'$.

Aus den obigen Gleichungen folgt nun durch Umkehrung, daß die n Produkte $k\omega_1$, $k\omega_2 \cdots k\omega_n$ der Ordnung $\mathfrak{o}'$ angehören, und folglich ist das Hauptideal $\mathfrak{o}k$ teilbar durch $\mathfrak{o}'$. Da ferner der größte gemeinschaftliche Teiler von je zwei durch $\mathfrak{o}'$ teilbaren Idealen selbst wieder ein durch $\mathfrak{o}'$ teilbares Ideal ist, so gibt es unter diesen, durch

$\mathfrak{o}'$ teilbaren Idealen ein einziges, völlig bestimmtes Ideal $\mathfrak{k}$ von kleinster Norm, und die genannten Ideale sind (nach § 1, 10°) identisch mit den sämtlichen Produkten $\mathfrak{a}\mathfrak{k}$, wo $\mathfrak{a}$ alle Ideale durchläuft. Dieses Ideal $\mathfrak{k}$ soll der Führer der Ordnung $\mathfrak{o}'$ heißen. Da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{o}'$ und folglich auch durch $\mathfrak{k}$ teilbar ist, so ist k^n als Norm von $\mathfrak{o}k$ teilbar durch

$$N(\mathfrak{k}) = (\mathfrak{o}, \mathfrak{k}) = (\mathfrak{o}, \mathfrak{o}')(\mathfrak{o}', \mathfrak{k}) = k(\mathfrak{o}', \mathfrak{k}).$$

Ist der Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ und für jede der $(\mathfrak{o}', \mathfrak{k})$ Zahlklassen, aus denen $\mathfrak{o}'$ besteht, ein Repräsentant gegeben, so ist $\mathfrak{o}'$ vollständig definiert. Nicht jedes Ideal $\mathfrak{k}$ kann der Führer einer Ordnung sein, sondern hierzu ist eine gewisse Bedingung erforderlich, deren Auffindung keine großen Schwierigkeiten darbietet; doch würde die Ableitung derselben sowie ein näheres Eingehen auf die Konstitution der Ordnungen überhaupt, uns hier zu weit führen. Das Gebiet $\mathfrak{o}$ ist offenbar selbst eine Ordnung und auch zugleich der Führer derselben.

§ 4.

Ideale der Ordnung $\mathfrak{o}'$.

Es sei nun $\mathfrak{o}'$ eine bestimmte Ordnung im Körper Ω, und $\mathfrak{k}$ der Führer derselben, so wollen wir ein System $\mathfrak{a}'$ von unendlich vielen Zahlen ein Ideal der Ordnung $\mathfrak{o}'$ oder kürzer ein Ideal in $\mathfrak{o}'$ nennen, wenn es die folgenden drei Bedingungen erfüllt:

I. Die Summen und Differenzen von je zwei in $\mathfrak{a}'$ enthaltenen Zahlen gehören ebenfalls dem System $\mathfrak{a}'$ an, d. h. $\mathfrak{a}'$ ist ein Modul im allgemeinsten Sinne des Wortes.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{a}'$ und aus einer Zahl der Ordnung $\mathfrak{o}'$ ist eine Zahl des Systems $\mathfrak{a}'$; d. h. $\mathfrak{o}'\mathfrak{a}'$ ist teilbar durch $\mathfrak{a}'$ und folglich auch $= \mathfrak{a}'$, weil $\mathfrak{o}'$ ein Teiler von [1] ist.

III. Der größte gemeinschaftliche Teiler $\mathfrak{a}' + \mathfrak{k}$ von $\mathfrak{a}'$ und $\mathfrak{k}$ ist $= \mathfrak{o}'$.

Für den Fall, daß die Ordnung $\mathfrak{o}'$ identisch mit $\mathfrak{o}$ ist, geht diese Definition eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ vollständig in die frühere Definition (§ 1, 1°) eines Ideals über, da die dritte Bedingung nur darauf hinauskommt, daß $\mathfrak{a}'$ durch $\mathfrak{o}$ teilbar ist. Wir werden daher diese Ideale künftig, wenn Mißverständnisse zu befürchten sind, Ideale in $\mathfrak{o}$ zu nennen haben. Im folgenden nehmen wir immer an, daß $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist.

Ist nun α' eine beliebige, aber von 0 verschiedene Zahl in $\mathfrak{a}'$, und bilden die n Zahlen $\omega_1', \omega_2' \cdots \omega_n'$ eine Basis der Ordnung $\mathfrak{o}'$, so sind die n Produkte $\alpha'\omega_1', \alpha'\omega_2', \cdots \alpha'\omega_n'$, welche (zufolge II) in $\mathfrak{a}'$ enthalten sind, voneinander unabhängig und bilden folglich eine Basis des Körpers Ω; mithin kann jede Zahl des Körpers durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Ideals $\mathfrak{a}'$ verwandelt werden, woraus wieder leicht folgt, daß $\mathfrak{a}'$ ein endlicher Modul $[\alpha_1', \alpha_2' \cdots \alpha_n']$, also ein Modul in dem Sinne des § 3 ist. Die Basiszahlen haben die Form

$$\begin{aligned}
\alpha_1' &= a_1'\omega_1' + a_2'\omega_2' + \cdots + a_n'\omega_n', \\
\alpha_2' &= a_1''\omega_1' + a_2''\omega_2' + \cdots + a_n''\omega_n', \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n' &= a_1^{(n)}\omega_1' + a_2^{(n)}\omega_2' + \cdots + a_n^{(n)}\omega_n',
\end{aligned}$$

wo die Koeffizienten ganze rationale Zahlen sind, deren Determinante

$$\sum \pm a_1' a_2'' \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}')$$

die Norm des Ideals $\mathfrak{a}'$ heißen und mit $N'(\mathfrak{a}')$ bezeichnet werden soll.

Es ergibt sich ferner leicht, daß $\mathfrak{o}'$ auch die Ordnung des Ideals $\mathfrak{a}'$ ist; in der Tat besteht die letztere, die wir mit $\mathfrak{o}_1$ bezeichnen wollen, zufolge ihrer Definition (§ 2, 6°) aus allen Zahlen ω_1, für welche $\mathfrak{a}'\omega_1 > \mathfrak{a}'$ wird, und da (nach II) $\mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'$ ist, so ist jedenfalls $\mathfrak{o}' > \mathfrak{o}_1$, und es braucht nur noch bewiesen zu werden, daß umgekehrt auch $\mathfrak{o}_1 > \mathfrak{o}'$ ist. Da nun $\mathfrak{a}'$ ein endlicher Modul des Körpers, und folglich (nach § 3, 1° und 2°) $[1] > \mathfrak{o}_1 > \mathfrak{o}$ ist, so ergibt sich $\mathfrak{k}[1] > \mathfrak{k}\mathfrak{o}_1 > \mathfrak{k}\mathfrak{o}$, mithin $\mathfrak{k}\mathfrak{o}_1 = \mathfrak{k}$, weil $\mathfrak{k}[1] = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$ ist; da außerdem (nach § 2, 6°) $\mathfrak{a}'\mathfrak{o}_1 = \mathfrak{a}'$, und (nach III) $\mathfrak{o}' = \mathfrak{k} + \mathfrak{a}'$ ist, so folgt $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{k}\mathfrak{o}_1 + \mathfrak{a}'\mathfrak{o}_1 = \mathfrak{k} + \mathfrak{a}'$, also $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{o}'$; nun ist aber $[1] > \mathfrak{o}'$, also auch $[1]\mathfrak{o}_1 > \mathfrak{o}'\mathfrak{o}_1$, d. h. $\mathfrak{o}_1 > \mathfrak{o}'$, was zu beweisen war.

Sind ferner $\mathfrak{a}'$, $\mathfrak{b}'$ zwei beliebige Ideale in $\mathfrak{o}'$, so überzeugt man sich leicht, daß $\mathfrak{a}' - \mathfrak{b}'$, $\mathfrak{a}' + \mathfrak{b}'$, $\mathfrak{a}'\mathfrak{b}'$ ebenfalls Ideale in $\mathfrak{o}'$ sind, und daß $\mathfrak{a}'\mathfrak{b}'$ sowohl durch $\mathfrak{a}'$ als durch $\mathfrak{b}'$ teilbar ist. Der Kürze wegen beschränke ich mich auf die Betrachtung des Produkts. Da $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, so ergibt sich $\mathfrak{o}'(\mathfrak{a}'\mathfrak{b}') = (\mathfrak{o}'\mathfrak{a}')\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}'$, also besitzt $\mathfrak{a}'\mathfrak{b}'$ die Eigenschaft II. Da ferner $\mathfrak{b}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$ ist, so folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{a}'$; ebenso ist $\mathfrak{a}'\mathfrak{b}'$ durch $\mathfrak{b}'$ teilbar. Da endlich $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ ist, so folgt $\mathfrak{b}' = \mathfrak{o}'\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}'$, also $\mathfrak{o}' = \mathfrak{b}' + \mathfrak{k} = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}' + \mathfrak{k}$; da nun $\mathfrak{k} = \mathfrak{k}\mathfrak{o}$, und $\mathfrak{b}' > \mathfrak{o}$ ist, so folgt $\mathfrak{k}\mathfrak{b}' + \mathfrak{k} = \mathfrak{k}(\mathfrak{b}' + \mathfrak{o}) = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$, also $\mathfrak{o}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}$, womit auch die Eigenschaft III für $\mathfrak{a}'\mathfrak{b}'$ dargetan ist.

§ 5.

Korrespondenz zwischen den Idealen in $\mathfrak{o}'$ und $\mathfrak{o}$.

Man könnte nun eine Theorie der Ideale in $\mathfrak{o}'$ aufstellen, welche sowohl in den Sätzen wie in ihren Beweisen eine vollständige Analogie mit der früheren Theorie der Ideale in $\mathfrak{o}$ darbieten würde. Allein es ist viel bequemer, die neue Theorie auf die alte zurückzuführen. Dies geschieht durch die folgenden Sätze.

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, so ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{k}$; zugleich ist $\mathfrak{a}'$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}'$ und $\mathfrak{o}\mathfrak{a}'$, und folglich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Ist ferner $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$, so ist $\mathfrak{a}' = \mathfrak{b}'$.

Beweis. Der Modul $\mathfrak{o}\mathfrak{a}'$ genügt der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{a}') = \mathfrak{o}\mathfrak{a}'$, weil $\mathfrak{o}^2 = \mathfrak{o}$ ist, und er ist teilbar durch $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $[1] > \mathfrak{o}' > \mathfrak{o}$ ist; also ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$. Aus $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ folgt durch Multiplikation mit $\mathfrak{o}$ ferner $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{k}$, also sind $\mathfrak{o}\mathfrak{a}'$ und $\mathfrak{k}$ relative Primideale. Hieraus ergibt sich ferner (entweder nach der bekannten Theorie der Ideale in $\mathfrak{o}$, oder auch unmittelbar), daß ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{k} - \mathfrak{o}\mathfrak{a}' = \mathfrak{k}\mathfrak{o}\mathfrak{a}' = \mathfrak{k}\mathfrak{a}'$ ist. Wendet man nun den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{b} = \mathfrak{k}$, $\mathfrak{c} = \mathfrak{o}\mathfrak{a}'$ an, so ergibt sich, weil $\mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = (\mathfrak{o}' + \mathfrak{o})\mathfrak{a}' = \mathfrak{o}\mathfrak{a}'$ ist,

$$\begin{aligned}\mathfrak{o}' - \mathfrak{o}\mathfrak{a}' &= \mathfrak{a}' + (\mathfrak{k} - \mathfrak{o}\mathfrak{a}') = \mathfrak{a}' + \mathfrak{k}\mathfrak{a}' \\ &= \mathfrak{a}'(\mathfrak{o}' + \mathfrak{k}) = \mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'.\end{aligned}$$

Ferner ist

$$\mathfrak{o}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{k} + \mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{k} + \mathfrak{o}\mathfrak{a}' = \mathfrak{o}.$$

Hieraus ergibt sich (nach § 2, 2°)

$$(\mathfrak{o}', \mathfrak{o}\mathfrak{a}') = (\mathfrak{o}', \mathfrak{a}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{a}'),$$

also $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Aus $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$ folgt endlich, weil $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{a}'$ und $\mathfrak{b}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{b}'$ ist, auch $\mathfrak{a}' = \mathfrak{b}'$, was zu beweisen war.

2°. Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{k}$, so ist das kleinste gemeinschaftliche Vielfache $\mathfrak{a}'$ von $\mathfrak{o}'$, $\mathfrak{a}$ ein Ideal in $\mathfrak{o}'$, und zugleich ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$.

Beweis. Zunächst ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}\mathfrak{a} = \mathfrak{a}$, weil $\mathfrak{o}' > \mathfrak{o}$, $\mathfrak{a}' > \mathfrak{a}$ ist; außerdem ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}'$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{o}' = \mathfrak{o}'$ ist; mithin ist

$\mathfrak{o}'\mathfrak{a}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$ und folglich auch teilbar durch $\mathfrak{a}'$, d. h. $\mathfrak{a}'$ genügt der Bedingung II. Nach einem für drei beliebige Moduln $\mathfrak{a}$, $\mathfrak{k}$, $\mathfrak{o}'$ geltenden Satze (§ 2, 1°) ist ferner

$$(\mathfrak{o}' - \mathfrak{a}) + (\mathfrak{o}' - \mathfrak{k}) = \mathfrak{o}' - (\mathfrak{a} + (\mathfrak{o}' - \mathfrak{k})),$$

und da in unserem Falle $\mathfrak{o}' - \mathfrak{a} = \mathfrak{a}'$, $\mathfrak{o}' - \mathfrak{k} = \mathfrak{k}$, $\mathfrak{a} + \mathfrak{k} = \mathfrak{o}$, $\mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$ ist, so ergibt sich $\mathfrak{a}' + \mathfrak{k} = \mathfrak{o}'$, also genügt $\mathfrak{a}'$ auch der Bedingung III und ist folglich ein Ideal in $\mathfrak{o}'$. Hieraus folgt (nach dem Satze 1°), daß $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{k}$, also auch $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'\mathfrak{a} + \mathfrak{k}\mathfrak{a}$ ist; da nun $\mathfrak{a}$, $\mathfrak{k}$ Ideale in $\mathfrak{o}$ sind, so ist $\mathfrak{k}\mathfrak{a} > \mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{a} > \mathfrak{a}$, also muß $\mathfrak{k}\mathfrak{a}$, als gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$, durch $\mathfrak{a}'$ und folglich auch durch $\mathfrak{o}\mathfrak{a}'$ teilbar sein; da nun auch $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ durch $\mathfrak{o}\mathfrak{a}'$ teilbar, also $\mathfrak{o}\mathfrak{a}'$ ein gemeinschaftlicher Teiler von $\mathfrak{k}\mathfrak{a}$ und $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ ist, so folgt, daß $\mathfrak{a}$ als größter gemeinschaftlicher Teiler von $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ und $\mathfrak{k}\mathfrak{a}$ gewiß durch $\mathfrak{o}\mathfrak{a}'$ teilbar ist; umgekehrt ist aber auch $\mathfrak{o}\mathfrak{a}' > \mathfrak{a}$, weil $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ ist; mithin ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$, was zu beweisen war.

Durch diese beiden Sätze ist eine eindeutige, gegenseitige Korrespondenz zwischen allen Idealen $\mathfrak{a}'$ in $\mathfrak{o}'$ und allen denjenigen Idealen $\mathfrak{a}$ in $\mathfrak{o}$ begründet, welche relative Primideale zum Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ sind; die Korrespondenz zwischen $\mathfrak{a}$ und $\mathfrak{a}'$ besteht darin, daß gleichzeitig $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'$, und $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ ist. Offenbar entsprechen sich auf diese Weise die beiden Ideale $\mathfrak{o}$ und $\mathfrak{o}'$.

Es ist schon oben (§ 4) bewiesen, daß jedes Produkt $\mathfrak{a}'\mathfrak{b}'$ aus zwei Idealen $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ wieder ein Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$, und zwar durch $\mathfrak{a}'$ und durch $\mathfrak{b}'$ teilbar ist; da nun $\mathfrak{o}^2 = \mathfrak{o}$ ist, so ist gleichzeitig $\mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}' = \mathfrak{o}\mathfrak{c}'$, also (nach § 1, 9°) $N(\mathfrak{o}\mathfrak{a}'\mathfrak{b}') = N(\mathfrak{o}\mathfrak{a}')N(\mathfrak{o}\mathfrak{b}')$ und folglich auch

$$N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}').$$

Umgekehrt: wenn $\mathfrak{a}'$, $\mathfrak{c}'$ Ideale in $\mathfrak{o}'$ sind, und wenn $\mathfrak{c}'$ durch $\mathfrak{a}'$ teilbar ist, so ist auch $\mathfrak{o}\mathfrak{c}' > \mathfrak{o}\mathfrak{a}'$, und folglich (§ 1, 10°) gibt es ein und nur ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$, für welches $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}$ wird; da nun $\mathfrak{o}\mathfrak{c}'$, also auch $\mathfrak{b}$, relatives Primideal zu $\mathfrak{k}$ ist, so gibt es (nach 2°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$, für welches $\mathfrak{o}\mathfrak{b}' = \mathfrak{b}$ wird; es ist daher $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$, woraus (nach 1°) $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ folgt; wäre nun zugleich $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ und $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, so würde $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}'$, und hieraus (nach § 1, 10°) $\mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{b}'$, also auch $\mathfrak{b}' = \mathfrak{b}'$ folgen. Hiermit ist folgender Satz bewiesen:

3^0. Ist das Ideal c' in o' teilbar durch das Ideal a' in o', so gibt es ein und nur ein Ideal b' in o' von der Art, daß $a'b' = c'$ wird; außerdem ist immer $N'(a'b') = N'(a')N'(b')$.

Aus allem diesen ergibt sich ohne weiteres, daß die Gesetze der Teilbarkeit der Ideale in o' und ihrer Multiplikation gänzlich mit den Gesetzen der Teilbarkeit derjenigen Ideale in o, welche relative Primideale zu $\mathfrak{k}$ sind, übereinstimmen und durch die genannte Korrespondenz aus den letzteren unmittelbar entnommen werden.

§ 6.

Hauptideale und Ideal-Klassen in o'.

Zwei Moduln a, b des Körpers Ω, d. h. endliche Moduln, deren Basen zugleich Basen des Körpers sind (§ 3), sollen äquivalent heißen, wenn es eine Zahl μ von der Beschaffenheit gibt, daß $a\mu = b$, und folglich, da μ nicht verschwinden kann, auch $b\mu^{-1} = a$ wird. Offenbar muß μ eine Zahl des Körpers Ω sein, und wir wollen dem vorstehenden Begriff der Äquivalenz noch die Beschränkung hinzufügen, daß a, b nur dann äquivalent heißen sollen, wenn eine Zahl μ von der genannten Beschaffenheit existiert, deren Norm zugleich positiv ist; wenn aber der Bedingung $a\mu = b$ nur durch solche Zahlen μ genügt werden kann, deren Normen negativ sind, so können a, b halb-äquivalent genannt werden. Sind zwei Moduln b, c mit einem dritten a äquivalent, so sind b, c offenbar auch miteinander äquivalent. Man kann daher die Moduln des Körpers Ω in Modul-Klassen einteilen, deren jede aus allen den Moduln besteht, welche mit einem bestimmten Modul, dem Repräsentanten der Klasse, äquivalent sind. Alle Moduln einer Klasse besitzen dieselbe Ordnung o', welche die Ordnung der Klasse heißen soll; denn wenn $a\mu = b$, und ω' irgend eine Zahl ist, für welche $a\omega' > a$ wird, so folgt durch Multiplikation mit μ oder $[\mu]$, daß auch $b\omega' > b$ ist, und umgekehrt ergibt sich hieraus wieder $a\omega' > a$. Durchläuft a alle Moduln einer Klasse A, ebenso b alle Moduln einer Klasse B, so gehören offenbar alle Produkte ab einer und derselben Klasse an, welche die aus A, B zusammengesetzte Klasse oder das Produkt aus A, B heißen und mit AB bezeichnet werden soll.

Wir beschränken uns aber hier auf die Betrachtung der Ideale und verstehen unter einer Ideal-Klasse der Ordnung o' den Inbegriff A' aller Ideale in o', welche mit einem bestimmten Ideal a'

in $\mathfrak{o}'$ äquivalent sind. Jedes mit $\mathfrak{o}'$ selbst äquivalente Ideal soll ein Hauptideal in $\mathfrak{o}'$, und der Inbegriff aller dieser Hauptideale soll die Hauptklasse in $\mathfrak{o}'$ heißen und mit O' bezeichnet werden. Ein solches Hauptideal ist daher von der Form $\mathfrak{o}'\mu$, wo μ in $\mathfrak{o}'$ enthalten ist, weil $\mathfrak{o}'\mu$ durch $\mathfrak{o}'$ teilbar sein muß; außerdem muß das zugehörige Ideal $\mathfrak{o}\mathfrak{o}'\mu = \mathfrak{o}\mu$ relatives Primideal zu $\mathfrak{k}$, d. h. μ muß relative Primzahl zu $\mathfrak{k}$ sein (D. § 163, 7.). Umgekehrt, ist die in $\mathfrak{o}'$ enthaltene Zahl μ relative Primzahl zu $\mathfrak{k}$, und ist $N(\mu) > 0$, so ist $\mathfrak{o}'\mu$ offenbar ein Hauptideal in $\mathfrak{o}'$. Nun besteht folgender Satz, von welchem wichtige Anwendungen zu machen sind:

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, und $\mathfrak{n}'$ ein durch $\mathfrak{o}'$ teilbarer Modul, welcher der Bedingung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$ genügt, so gibt es immer ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$, und $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ wird.

Beweis. Der Modul $\mathfrak{o}\mathfrak{n}'$ ist ein Ideal in $\mathfrak{o}$, weil er durch $\mathfrak{o}$ teilbar ist und der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{n}') = \mathfrak{o}\mathfrak{n}'$ genügt. Man zerlege nun $\mathfrak{o}\mathfrak{n}'$ in seine sämtlichen Primideal-Faktoren (§ 1, 12°) und bezeichne mit $\mathfrak{k}_1$ das Produkt aller derjenigen dieser Primideale, welche in $\mathfrak{k}$ aufgehen, mit $\mathfrak{n}_1$ das Produkt aller übrigen, so daß $\mathfrak{o}\mathfrak{n}' = \mathfrak{k}_1\mathfrak{n}_1$ wird. Nun gibt es (§ 1, 14° oder D. § 163, 7.) immer ein Ideal $\mathfrak{m}_1$ in $\mathfrak{o}$ von der Art, daß $\mathfrak{o}\mathfrak{a}'\mathfrak{m}_1 = \mathfrak{a}'\mathfrak{m}_1 = \mathfrak{o}\alpha$, d. h. ein Hauptideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{m}_1 + \mathfrak{n}_1 = \mathfrak{o}$, also $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$ wird. Da ferner $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, also $\mathfrak{o}\mathfrak{a}'$ relatives Primideal zu $\mathfrak{k}$ ist, so sind auch $\mathfrak{o}\mathfrak{a}'\mathfrak{n}_1 = \mathfrak{a}'\mathfrak{n}_1$ und $\mathfrak{k}\mathfrak{k}_1$ relative Primideale, und folglich (§ 2, 2° oder D. § 163, 7.) gibt es Zahlen μ, welche den beiden gleichzeitigen Kongruenzen

$$\mu \equiv \alpha \pmod{\mathfrak{a}'\mathfrak{n}_1}, \quad \mu \equiv 1 \pmod{\mathfrak{k}\mathfrak{k}_1}$$

genügen; diese Zahlen μ bilden eine bestimmte Zahl-Klasse in bezug auf den Modul $\mathfrak{a}'\mathfrak{n}_1\mathfrak{k}\mathfrak{k}_1 = \mathfrak{k}\mathfrak{a}'\mathfrak{n}'$, und man kann, wie unten nachträglich bewiesen werden soll, die Zahl μ zugleich so wählen, daß $N(\mu) > 0$ wird. Aus der zweiten der beiden vorstehenden Kongruenzen folgt nun, daß μ relative Primzahl zu $\mathfrak{k}\mathfrak{k}_1$ und folglich auch zu $\mathfrak{k}$ ist; da ferner $\mathfrak{k}\mathfrak{k}_1 > \mathfrak{k} > \mathfrak{o}'$, und da die Zahl 1 in der Ordnung $\mathfrak{o}'$ enthalten ist, so ist zufolge der zweiten Kongruenz auch μ in $\mathfrak{o}'$ enthalten, und folglich ist $\mathfrak{o}'\mu$ ein Hauptideal in $\mathfrak{o}'$. Aus der ersten Kongruenz folgt ferner mit Rücksicht auf $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, daß auch $\mathfrak{o}\mu + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, und folglich $\mathfrak{o}\mu = \mathfrak{o}\mathfrak{a}'\mathfrak{b} = \mathfrak{a}'\mathfrak{b}$ ist, wo $\mathfrak{b}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{n}_1$ ist. Da ferner $\mathfrak{o}\mu$, und

folglich auch $\mathfrak{b}$ relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1$ ist, so ist $\mathfrak{b}$ auch relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1\mathfrak{n}_1 = \mathfrak{k}\mathfrak{n}'$, also $\mathfrak{b} + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}$. Bedeutet ferner $\mathfrak{b}'$ das dem Ideal $\mathfrak{b}$ entsprechende Ideal in $\mathfrak{o}'$ (§ 5), so ist $\mathfrak{b} = \mathfrak{o}\mathfrak{b}'$, und aus $\mathfrak{o}\mu = \mathfrak{a}'\mathfrak{b}$, d. h. aus $\mathfrak{o}(\mathfrak{o}'\mu) = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$ folgt $\mathfrak{o}'\mu = \mathfrak{a}'\mathfrak{b}'$. Nun ist $\mathfrak{k} > \mathfrak{o}'$ und nach Voraussetzung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$, folglich $\mathfrak{k}\mathfrak{n}' > \mathfrak{n}'$, und da ebenfalls $\mathfrak{n}' > \mathfrak{o}'$ vorausgesetzt ist, so folgt $\mathfrak{k}\mathfrak{n}' > \mathfrak{o}'$, also $\mathfrak{o}' - \mathfrak{k}\mathfrak{n}' = \mathfrak{k}\mathfrak{n}'$; wendet man daher den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{o}'$, $\mathfrak{c} = \mathfrak{k}\mathfrak{n}'$ an und berücksichtigt außerdem, daß $\mathfrak{o}' - \mathfrak{b} = \mathfrak{b}'$, und $\mathfrak{b} + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}$ ist, so folgt $\mathfrak{b}' + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$, woraus mit Rücksicht auf $\mathfrak{k}\mathfrak{n}' > \mathfrak{n}' > \mathfrak{o}'$ sich endlich auch $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ ergibt, was zu beweisen war.

Es ist nun noch der oben vorläufig übergangene Beweis nachzuholen, daß man μ so wählen kann, daß $N(\mu)$ positiv wird. Dies geschieht offenbar durch den Beweis des folgenden allgemeineren Satzes:

2°. Ist $\mathfrak{m}$ ein Modul des Körpers Ω, und μ_0 eine bestimmte Zahl dieses Körpers, so gibt es unter den Zahlen μ, welche $\equiv \mu_0 \pmod{\mathfrak{m}}$ sind, unendlich viele, die eine positive Norm haben.

Beweis. Dieser Satz ist selbstverständlich, sobald die sämtlichen Wurzeln der Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω abgeleitet ist, imaginär, und folglich die n Faktoren von $N(\mu) = \mu'\mu'' \cdots \mu^{(n)}$ aus $\frac{1}{2}n$ Paaren von zwei Zahlen $a + bi$, $a - bi$ bestehen; und wenn die Gleichung eine oder mehrere reelle Wurzeln hat, so braucht man offenbar nur die diesen Wurzeln entsprechenden Faktoren von $N(\mu)$ zu betrachten, weil das Produkt der übrigen gewiß positiv ist. Da nun nach Voraussetzung die Basiszahlen des endlichen Moduls $\mathfrak{m}$ zugleich eine Basis des Körpers Ω bilden, so kann die dem Körper angehörende Zahl 1 durch Multiplikation mit einer positiven rationalen Zahl m in eine Zahl m des Moduls $\mathfrak{m}$ verwandelt werden, und wenn h eine beliebige ganze rationale Zahl bedeutet, so wird $hm \equiv 0 \pmod{\mathfrak{m}}$, und folglich $\mu = \mu_0 + hm \equiv \mu_0 \pmod{\mathfrak{m}}$. Offenbar kann man nun die ganze rationale Zahl h positiv und so groß wählen, daß diejenigen Faktoren

$$\mu' = \mu_0' + hm, \quad \mu'' = \mu_0'' + hm \cdots \mu^{(n)} = \mu_0^{(n)} + hm,$$

welche den reellen Wurzeln der Gleichung $f(\Theta) = 0$ entsprechen, sämtlich positiv ausfallen, womit der Satz bewiesen ist.

§ 7.

Komposition der Ideal-Klassen.

Sind $\mathfrak{o}'$, $\mathfrak{o}''$ zwei beliebige Ordnungen des Körpers Ω, und $\mathfrak{f}'$, $\mathfrak{f}''$ ihre Führer, so ist offenbar ihr Produkt $\mathfrak{o}''' = \mathfrak{o}'\mathfrak{o}''$ ebenfalls eine Ordnung (§ 3), und da $\mathfrak{o}'''$ ein gemeinschaftlicher Teiler von $\mathfrak{o}'$, $\mathfrak{o}''$ ist, so muß der Führer $\mathfrak{f}'''$ der Ordnung $\mathfrak{o}'''$ auch ein gemeinschaftlicher Teiler von $\mathfrak{f}'$, $\mathfrak{f}''$ sein. Ist nun $\mathfrak{a}'$ ein beliebiges Ideal in $\mathfrak{o}'$, ebenso $\mathfrak{b}''$ ein beliebiges Ideal in $\mathfrak{o}''$, so wird $\mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$ ein Ideal in $\mathfrak{o}'''$; denn aus $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, $\mathfrak{o}''\mathfrak{b}'' = \mathfrak{b}''$ folgt $\mathfrak{o}'''\mathfrak{c}''' = \mathfrak{o}'\mathfrak{o}''\mathfrak{a}'\mathfrak{b}'' = \mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$; aus $\mathfrak{a}' + \mathfrak{f}' = \mathfrak{o}'$, $\mathfrak{b}'' + \mathfrak{f}'' = \mathfrak{o}''$ ergibt sich ferner durch Multiplikation

$$\mathfrak{a}'\mathfrak{b}'' + \mathfrak{a}'\mathfrak{f}'' + \mathfrak{f}'\mathfrak{b}'' + \mathfrak{f}'\mathfrak{f}'' = \mathfrak{o}'''$$

und hieraus, weil jedes der Ideale $\mathfrak{a}'\mathfrak{f}''$, $\mathfrak{f}'\mathfrak{b}''$, $\mathfrak{f}'\mathfrak{f}''$ durch $\mathfrak{f}'''$, und $\mathfrak{f}'''$ durch $\mathfrak{o}'''$ teilbar ist, $\mathfrak{a}'\mathfrak{b}'' + \mathfrak{f}''' = \mathfrak{o}'''$; also besitzt der Modul $\mathfrak{a}'\mathfrak{b}''$ die charakteristischen Eigenschaften eines Ideals in $\mathfrak{o}'''$ (§ 4), und da allgemein bewiesen ist, daß die Ordnung eines Ideals in $\mathfrak{o}'$ identisch mit $\mathfrak{o}'$ ist, so ergibt sich, daß die Ordnung eines Produkts von Idealen gleich dem Produkt aus den Ordnungen der Faktoren ist*).

Ist $\mathfrak{a}'$ ein Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$, und $\mathfrak{b}''$ ein Repräsentant der Ideal-Klasse B'' in $\mathfrak{o}''$, so ist jedes Produkt von zwei beliebigen Idealen in A', B'' von der Form $\mathfrak{a}'\mu \cdot \mathfrak{b}''\nu = \mathfrak{a}'\mathfrak{b}''(\mu\nu)$, also ein mit $\mathfrak{a}'\mathfrak{b}''$ äquivalentes Ideal; alle diese Produkte gehören daher einer und derselben Ideal-Klasse in $\mathfrak{o}'''$ an, welche (wie bei den Moduln) die aus A', B'' zusammengesetzte Klasse oder das Produkt aus A', B'' heißen und mit $A'B''$ bezeichnet werden soll. Bedeuten A, B, C beliebige Ideal-Klassen beliebiger Ordnungen, so ist offenbar $AB = BA$, $(AB)C = A(BC)$.

Von dieser allgemeinsten Komposition der Ideal-Klassen aller Ordnungen kehren wir zurück zu der Betrachtung der Ideal-Klassen einer einzigen Ordnung $\mathfrak{o}'$; jedes Produkt von solchen Klassen gehört derselben Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{o}'^2 = \mathfrak{o}'$ ist. Da das Produkt $\mathfrak{o}'\mu \cdot \mathfrak{a}' = \mu\mathfrak{a}'$ aus einem Hauptideal $\mathfrak{o}'\mu$ und einem beliebigen Ideal $\mathfrak{a}'$

*) Wenn, wie es bei den quadratischen Körpern der Fall ist, jede Modul-Klasse auch Ideale enthält, so gilt der obige Satz auch für Produkte aus Moduln; aber schon bei kubischen Körpern gibt es Moduln, welche keinem Ideale äquivalent sind, und der obige Satz darf nicht mehr auf alle Produkte von Moduln übertragen werden. Auf diese wichtige Frage werde ich bei einer anderen Gelegenheit zurückkommen.

mit diesem letzteren äquivalent ist, so folgt $O'A' = A'$, wo A' eine beliebige Ideal-Klasse in $\mathfrak{o}'$, und O' die Hauptklasse in $\mathfrak{o}'$ bedeutet. Da ferner, wenn $\mathfrak{a}'$ ein beliebiger Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$ ist, immer ein solches Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ existiert, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$ wird, so gibt es eine Ideal-Klasse B' in $\mathfrak{o}'$ von der Art, daß $A'B' = O'$ wird; und zwar gibt es nur eine einzige solche Klasse B'; denn wenn C' ebenfalls eine Ideal-Klasse in $\mathfrak{o}'$, und wenn $AC' = O'$ ist, so folgt $A'B'C' = O'B' = O'C' = B' = C'$. Diese Klasse B' soll die zu A' gehörende entgegengesetzte, oder die reziproke, oder inverse Klasse heißen und durch A'^{-1} bezeichnet werden; offenbar ist A' zugleich die inverse Klasse von A'^{-1}. Sind nun A', B', C' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so folgt aus $A'B' = A'C'$ durch Multiplikation mit A'^{-1} stets $B' = C'$*). Sind ferner A', B' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so gibt es immer eine und nur eine Ideal-Klasse $C' = A'^{-1}B'$ der Ordnung $\mathfrak{o}'$, welche der Bedingung $A'C' = B'$ genügt.

§ 8.

Korrespondenz zwischen den Ideal-Klassen in $\mathfrak{o}$ und $\mathfrak{o}'$.

Ist $\mathfrak{o}$ wieder die aus allen ganzen Zahlen des Körpers Ω bestehende Ordnung, O die Klasse der Hauptideale in $\mathfrak{o}$, und $\mathfrak{o}'$ eine beliebige Ordnung, so wird durch jede bestimmte Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ eine bestimmte Ideal-Klasse $OA' = A$ der Ordnung $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$ erzeugt, z. B. O selbst durch die Hauptklasse O' der Ordnung $\mathfrak{o}'$. Umgekehrt, ist A eine Ideal-Klasse der Ordnung $\mathfrak{o}$, so gibt es in ihr immer einen Repräsentanten $\mathfrak{a}$, der relatives Primideal zum Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist (denn nach § 1, 14° oder § 6 oder D. § 163, 7. kann jedes Ideal der inversen Klasse A^{-1} durch Multiplikation mit einem solchen Ideal $\mathfrak{a}$ in ein Hauptideal verwandelt werden, und dies muß folglich in A enthalten sein); dann ist $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ das korrespondierende Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$ (§ 5, 2°), und wenn A' die Ideal-Klasse in $\mathfrak{o}'$ ist, welcher $\mathfrak{a}'$ angehört, so ist $OA' = A$; also wird jede Ideal-Klasse A der Ordnung $\mathfrak{o}$ durch mindestens eine Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ auf diese Weise erzeugt. Wir suchen nun zunächst alle Ideal-Klassen B' der Ordnung $\mathfrak{o}'$, welche dieselbe

*) Dieser Satz verliert, wie man leicht sieht, seine allgemeine Gültigkeit, wenn die Klassen A', B', C' nicht derselben Ordnung angehören.

Klasse A hervorbringen, so daß $OB' = OA'$ wird; hieraus folgt aber $OB'A'^{-1} = OO'$, also, wenn

$$B'A'^{-1} = M', \quad B' = M'A'$$

gesetzt wird,

$$OM' = O.$$

Umgekehrt, wenn M' eine der vorstehenden Bedingung genügende Ideal-Klasse der Ordnung o', und wenn $B' = M'A'$ ist, so ist auch wirklich $OB' = OA'$.

Der Komplex $\mathfrak{M}'$ aller dieser Ideal-Klassen M', unter denen sich auch O' und jede inverse Klasse M'^{-1} befindet, besitzt den Charakter einer Gruppe, insofern das Produkt von je zwei solchen Klassen M' offenbar wieder demselben Komplex $\mathfrak{M}'$ angehört. In den folgenden Paragraphen wird gezeigt werden, daß die Anzahl dieser Klassen M' eine endliche ist; wir wollen dieselbe mit m bezeichnen und zunächst ihre Bedeutung für das Problem nachweisen, welches den Hauptgegenstand dieser Abhandlung bildet. Ist A' eine bestimmte Ideal-Klasse in o', und durchläuft M' alle m Klassen der Gruppe $\mathfrak{M}'$, so bilden die sämtlichen Produkte $M'A'$ einen Komplex von Klassen der Ordnung o', der mit $\mathfrak{M}'A'$ bezeichnet werden mag; da aus $M'_1A' = M'_2A'$ auch $M'_1 = M'_2$ folgt (§ 7), so besteht ein solcher Komplex $\mathfrak{M}'A'$ aus m verschiedenen Klassen. Enthalten ferner zwei solche Komplexe $\mathfrak{M}'A'$, $\mathfrak{M}'B'$ eine und dieselbe Klasse $M'_1A' = M'_2B'$, so ist $B' = M'^{-1}_2 M'_1 A' = M'_3 A'$, wo $M'_3 = M'^{-1}_1 M'_1$ ebenfalls in $\mathfrak{M}'$ enthalten ist, und hieraus folgt offenbar, daß die sämtlichen m Klassen des Komplexes $\mathfrak{M}'B'$ mit denen von $\mathfrak{M}'A'$ vollständig übereinstimmen. Man kann daher alle Ideal-Klassen der Ordnung o' in lauter verschiedene solche Komplexe von der Form $\mathfrak{M}'A'$, $\mathfrak{M}'B' \cdots$ einteilen. Nun ist oben gezeigt, daß jede bestimmte Ideal-Klasse A der Ordnung o in der angegebenen Weise durch die sämtlichen m Klassen eines bestimmten solchen Komplexes $\mathfrak{M}'A'$, und durch keine andere Klasse der Ordnung o' erzeugt wird, und daß umgekehrt alle m Klassen eines solchen Komplexes durch Multiplikation mit O eine und nur eine Klasse A der Ordnung o erzeugen. Mithin ist die Anzahl aller dieser Komplexe identisch mit der Anzahl h der verschiedenen Ideal-Klassen der Ordnung o, deren Endlichkeit schon bewiesen ist (D. § 164, 2°), und zugleich ergibt sich, daß

$$h' = mh$$

die Anzahl aller verschiedenen Ideal-Klassen der Ordnung o' ist.

§ 9.

Bestimmung des Verhältnisses m der Klassen-Anzahlen h' und h.

Es sei M' eine bestimmte Klasse der Gruppe $\mathfrak{M}'$, und $\mathfrak{m}'$ ein bestimmter Repräsentant von M'. Da $OM' = O$ ist, so ist $\mathfrak{o}\mathfrak{m}'$ ein Hauptideal in $\mathfrak{o}$, also von der Form $\mathfrak{o}\mu$, wo μ eine ganze Zahl von positiver Norm, und zwar relative Primzahl zu $\mathfrak{k}$ ist, wo $\mathfrak{k}$ wieder den Führer der Ordnung $\mathfrak{o}'$ bedeutet. Umgekehrt, ist μ eine solche Zahl, so ist $\mathfrak{o}\mu$ ein Hauptideal in $\mathfrak{o}$ und relatives Primideal zu $\mathfrak{k}$, mithin gibt es (§ 5, 2°) ein und nur ein Ideal $\mathfrak{m}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, und wenn M' die durch $\mathfrak{m}'$ repräsentierte Ideal-Klasse in $\mathfrak{o}'$ bedeutet, so ist $OM' = O$; jeder bestimmten Zahl μ von der angegebenen Beschaffenheit entspricht daher auf diese Weise eine und nur eine Ideal-Klasse M', welche der Gruppe $\mathfrak{M}'$ angehört. Auf diese Korrespondenz bezieht sich der folgende Satz:

Sind μ, μ_1 ganze Zahlen von positiver Norm und relative Primzahlen zu $\mathfrak{k}$, so besteht die erforderliche und hinreichende Bedingung dafür, daß beiden Zahlen eine und dieselbe Klasse M' der Gruppe $\mathfrak{M}'$ entspreche, in der Kongruenz

$$\mu_1 \equiv \mu\varepsilon\omega' \pmod{\mathfrak{k}},$$

wo ε eine Einheit in $\mathfrak{o}$, und ω' eine in $\mathfrak{o}'$ enthaltene relative Primzahl zu $\mathfrak{k}$ bedeutet, deren Normen beide positiv sind.

Beweis. Ist $\mathfrak{m}' = \mathfrak{o}' - \mathfrak{o}\mu$ das Ideal in $\mathfrak{o}'$, welches dem Ideal $\mathfrak{o}\mu$ entspricht und folglich der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, so kann man, weil $\mathfrak{m}' + \mathfrak{k} = \mathfrak{o}'$ ist, eine Zahl μ' so wählen, daß $\mu' \equiv 0 \pmod{\mathfrak{m}'}$ und $\mu' \equiv 1 \pmod{\mathfrak{k}}$ wird (§ 2, 2°); auch leuchtet ein, daß zugleich die Bedingung $N(\mu') > 0$ erfüllt werden kann (§ 6, 2°). Dann ist $\mathfrak{o}'\mu'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal in $\mathfrak{o}'$, weil $\mathfrak{o}'\mu' + \mathfrak{k} = \mathfrak{o}'$ ist, und folglich gibt es ein Ideal $\mathfrak{n}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{m}'\mathfrak{n}' = \mathfrak{o}'\mu'$ genügt und folglich der inversen Klasse M'^{-1} angehört. Hieraus folgt durch Multiplikation mit $\mathfrak{o}$, daß $\mathfrak{o}\mu' = \mathfrak{o}\mathfrak{n}'\mu$, also μ' durch μ teilbar ist; setzt man $\mu' = \mu\nu$, so ist ν eine ganze Zahl von positiver Norm und relative Primzahl zu $\mathfrak{k}$, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{k}}$ ist; zugleich wird $\mathfrak{o}\mu\nu = \mathfrak{o}\mathfrak{n}'\mu$, und folglich $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$.

Wenn nun das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1' = \mathfrak{o}' - \mathfrak{o}\mu_1$ derselben Klasse M' angehört, wie $\mathfrak{m}'$, so ist auch $\mathfrak{m}_1'\mathfrak{n}'$ ein Hauptideal in $\mathfrak{o}'$, also $\mathfrak{m}_1'\mathfrak{n}' = \mathfrak{o}'\omega'$, wo ω' eine Zahl in $\mathfrak{o}'$ von positiver Norm und relative Primzahl zu $\mathfrak{f}$ ist. Multipliziert man mit $\mathfrak{o}$ und berücksichtigt, daß $\mathfrak{o}\mathfrak{m}_1' = \mathfrak{o}\mu_1$ und $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$ ist, so folgt $\mathfrak{o}\mu_1\nu = \mathfrak{o}\omega'$, und hieraus $\mu_1\nu = \varepsilon\omega'$, wo ε eine Einheit in $\mathfrak{o}$ bedeutet, deren Norm $= +1$ sein muß, weil die Normen der Zahlen μ_1, ν, ω' positiv sind. Multipliziert man mit μ, so ergibt sich die zu beweisende Kongruenz, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{f}}$ und $\mathfrak{o}\mathfrak{f} = \mathfrak{f}$ ist.

Umgekehrt, wenn diese Kongruenz, in welcher μ, μ_1, ε, ω' die in dem Satze angegebene Bedeutung haben, erfüllt ist, so folgt durch Multiplikation mit $\nu\varepsilon^{-1}$ die Kongruenz

$$\nu\mu_1\varepsilon^{-1} \equiv \omega' \pmod{\mathfrak{f}},$$

aus welcher hervorgeht, daß die ganze Zahl $\alpha' = \nu\mu_1\varepsilon^{-1}$, welche relative Primzahl zu $\mathfrak{f}$ ist und eine positive Norm besitzt, der Ordnung $\mathfrak{o}'$ angehört, und folglich ist $\mathfrak{o}'\alpha'$ ein Hauptideal in $\mathfrak{o}'$. Da nun $\mathfrak{o}\nu = \mathfrak{o}\mathfrak{n}'$ und $\mathfrak{o}\mu_1\varepsilon^{-1} = \mathfrak{o}\mu_1 = \mathfrak{o}\mathfrak{m}_1'$ ist, so folgt $\mathfrak{o}(\mathfrak{o}'\alpha') = \mathfrak{o}(\mathfrak{n}'\mathfrak{m}_1')$, also auch $\mathfrak{o}'\alpha' = \mathfrak{n}'\mathfrak{m}_1'$ (§ 5, 1°), mithin gehören die Ideale $\mathfrak{n}'$, $\mathfrak{m}_1'$ zu entgegengesetzten Klassen, d. h. das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1'$ ist äquivalent mit $\mathfrak{m}'$, was zu beweisen war.

Mit Hilfe dieses Satzes ist es leicht, die Anzahl m der in der Gruppe $\mathfrak{M}'$ enthaltenen Klassen M' zu bestimmen. Wir bezeichnen mit $\psi(\mathfrak{f})$ die Anzahl aller der in $\mathfrak{o}$ enthaltenen Zahlen ω, welche inkongruent in bezug auf den Modul $\mathfrak{f}$ und zugleich relative Primzahlen zu $\mathfrak{f}$ sind; diese Anzahl ist (D. § 163, 7.)

$$\psi(\mathfrak{f}) = N(\mathfrak{f}) \prod \left(1 - \frac{1}{N(\mathfrak{q})}\right),$$

wo das Produktzeichen Π sich auf alle verschiedenen, in $\mathfrak{f}$ aufgehenden Primideale $\mathfrak{q}$ bezieht. Die Repräsentanten ω selbst können (nach § 6, 2°) immer so gewählt werden, daß sie positive Normen haben. Wenn eine dieser Zahlen (wie z. B. die Zahl 1) in $\mathfrak{o}'$ enthalten ist, so gehören auch alle mit ihr kongruenten Zahlen der Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{f}$ durch $\mathfrak{o}'$ teilbar ist; die Anzahl dieser nach $\mathfrak{f}$ inkongruenten Zahlen ω' oder der zugehörigen Zahlklassen ist ebenfalls als bekannt anzusehen, sobald $\mathfrak{o}'$ gegeben ist, und soll mit $\psi'(\mathfrak{f})$ bezeichnet werden. Da $\mathfrak{o}'^2 = \mathfrak{o}'$ ist, so ist das Produkt aus je zwei Repräsentanten dieser Zahlklassen immer wieder einem solchen Re-

präsentanten kongruent, und der Komplex dieser $\psi'(\mathfrak{f})$ Repräsentanten hat daher den Charakter einer Gruppe. Multipliziert man dieselben mit einer beliebigen in $\mathfrak{o}$ enthaltenen Zahl ω, welche relative Primzahl zu $\mathfrak{f}$ ist, so erhält man $\psi'(\mathfrak{f})$ inkongruente Zahlen, welche ebenfalls relative Primzahlen zu $\mathfrak{f}$ sind, und deren Komplex kurz mit (ω) bezeichnet werden soll; zwei solche Komplexe (α), (β) sind (nach der in § 8 angewendeten Schlußweise) entweder gänzlich verschieden, d. h. keine der in (α) enthaltenen Zahlen ist kongruent mit einer der in (β) enthaltenen Zahlen, oder sie sind völlig identisch, d. h. alle durch den einen Komplex vertretenen $\psi'(\mathfrak{f})$ Zahlklassen stimmen gänzlich mit den Zahlklassen des anderen Komplexes überein. Es wird daher auch das System aller $\psi(\mathfrak{f})$ Repräsentanten in eine Anzahl solcher Komplexe (ω) zerfallen, d. h. $\psi(\mathfrak{f})$ wird teilbar sein durch $\psi'(\mathfrak{f})$; wir betrachten zunächst aber nur alle diejenigen Komplexe (ε), welche entstehen, wenn ε alle Einheiten des Gebietes $\mathfrak{o}$ durchläuft, deren Normen $= +1$ sind. Es sei s die Anzahl aller verschiedenen Komplexe

$$(\varepsilon_1),\ (\varepsilon_2) \cdots (\varepsilon_s)$$

dieser Art, so bilden die in ihnen enthaltenen $s\psi'(\mathfrak{f})$ Repräsentanten offenbar wieder eine Gruppe im obigen Sinne; jede Zahl von der Form $\varepsilon\omega'$ ist einer und nur einer dieser Zahlen kongruent, welche umgekehrt selbst in dieser Form enthalten sind. Ist nun μ eine in $\mathfrak{o}$ enthaltene relative Primzahl zu $\mathfrak{f}$, deren Norm positiv ist, und bezeichnet man mit $((\mu))$ den Komplex der $s\psi'(\mathfrak{f})$ inkongruenten, in den s Komplexen $(\mu\varepsilon_1)$, $(\mu\varepsilon_2) \cdots (\mu\varepsilon_s)$ enthaltenen Zahlen, so sind wieder zwei solche Komplexe $((\mu))$ und $((\mu_1))$ entweder gänzlich verschieden, oder völlig identisch, und folglich besteht das System aller $\psi(\mathfrak{f})$ Repräsentanten ω aus einer Anzahl von solchen Komplexen $((\mu))$; diese Anzahl muß aber notwendig $= m$, d. h. gleich der Anzahl der verschiedenen, in der Gruppe $\mathfrak{M}'$ enthaltenen Idealklassen M' sein, weil nach dem obigen Satze je zwei Hauptidealen $\mathfrak{o}\mu$, $\mathfrak{o}\mu_1$ dieselbe Klasse M' oder zwei verschiedene solche Klassen entsprechen, je nachdem die beiden Komplexe $((\mu))$, $((\mu_1))$ identisch oder verschieden sind. Mithin ist

$$\psi(\mathfrak{f}) = m s \psi'(\mathfrak{f}),$$

also

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{s\psi'(\mathfrak{f})}.$$

§ 10.

Umformung des Resultates.

Es ist nun noch von Wichtigkeit, die Anzahl s in bestimmter Weise darzustellen, und hierzu gelangt man mit Hilfe der in der Einleitung erwähnten Theorie der Einheiten von Dirichlet, welche ich zu diesem Zwecke in etwas verallgemeinerter Form dargestellt habe (D. § 166). Wir fragen zunächst: wie müssen zwei Einheiten $\varepsilon, \varepsilon_0$ von positiver Norm beschaffen sein, damit die oben mit (ε), (ε_0) bezeichneten Komplexe identisch ausfallen? Offenbar ist hierzu erforderlich, daß $\varepsilon \equiv \varepsilon_0 \omega' \pmod{\mathfrak{f}}$ sei, wo ω' eine der Ordnung $\mathfrak{o}'$ angehörende Zahl bedeutet; mithin muß $\varepsilon \varepsilon_0^{-1} \equiv \omega' \pmod{\mathfrak{f}}$, also $\varepsilon = \varepsilon' \varepsilon_0$ sein, wo $\varepsilon' = \varepsilon \varepsilon_0^{-1}$ eine der Ordnung $\mathfrak{o}'$ angehörende Einheit von positiver Norm bedeutet; und es leuchtet unmittelbar ein, daß diese Bedingung $\varepsilon = \varepsilon' \varepsilon_0$ auch hinreichend ist, daß sie also die Identität der Komplexe (ε), (ε_0) zur Folge hat. Bezeichnet man daher, wie oben, mit $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$ die sämtlichen s verschiedenen Komplexe von der Form (ε), so ergibt sich, daß man alle Einheiten ε der Ordnung $\mathfrak{o}$, und jede nur ein einziges Mal erhält, wenn man jede der s partikulären Einheiten $\varepsilon_1, \varepsilon_2 \cdots \varepsilon_s$ mit allen Einheiten ε' der Ordnung $\mathfrak{o}'$ multipliziert. Hieraus folgt zunächst, daß die s-te Potenz ε^s einer jeden Einheit ε in $\mathfrak{o}$ immer eine Einheit ε' in $\mathfrak{o}'$ ist, weil die s Komplexe $(\varepsilon \varepsilon_1), (\varepsilon \varepsilon_2) \cdots (\varepsilon \varepsilon_s)$ notwendig mit den Komplexen $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$, wenn auch in anderer Ordnung, übereinstimmen müssen, und weil folglich das Produkt

$$\varepsilon \varepsilon_1 \cdot \varepsilon \varepsilon_2 \cdots \varepsilon \varepsilon_s = \varepsilon^s \cdot \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$$

von der Form $\varepsilon' . \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$ ist, wo ε' eine Einheit der Ordnung $\mathfrak{o}'$ bedeutet.

Wir müssen nun das Hauptresultat der Theorie der Einheiten kurz in Erinnerung bringen. Es sei ν die Gesamtanzahl der $(2\nu - n)$ reellen Wurzeln und der $(n - \nu)$ Paare von je zwei konjugiert-imaginären Wurzeln $a \pm bi$ der irreduktiblen Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω entsprungen ist (§ 1); behält man von jedem Paare imaginärer Wurzeln nur die eine bei, so bleiben ν Wurzeln übrig, die mit

$$\Theta', \Theta'' \cdots \Theta^{(\nu)}$$

bezeichnet werden mögen. Ist nun $\varepsilon = \varphi(\Theta)$ eine beliebige Einheit des Körpers Ω, so soll durch das Symbol $l'(\varepsilon)$ der reelle Teil des

Logarithmen von $\varphi(\Theta')$ oder das Doppelte dieses reellen Teils bezeichnet werden, je nachdem Θ' reell oder imaginär ist, und die Symbole $l''(\varepsilon), l'''(\varepsilon) \cdots l^{(\nu)}(\varepsilon)$ sollen die entsprechende Bedeutung in bezug auf die anderen Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ haben. Dann folgt aus $N(\varepsilon) = 1$, daß immer

$$l'(\varepsilon) + l''(\varepsilon) + \cdots + l^{(\nu)}(\varepsilon) = 0$$

ist. Es wird nun zunächst bewiesen (D. § 166, 5.), daß es in jeder Ordnung $\mathfrak{o}'$ immer $(\nu - 1)$ voneinander **unabhängige**, d. h. solche Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ gibt, für welche die Determinante

$$\sum \pm l'(\varrho_1') l''(\varrho_2') \cdots l^{(\nu-1)}(\varrho_{\nu-1}'),$$

welche wir zur Abkürzung mit

$$L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$$

bezeichnen wollen, einen von 0 verschiedenen (positiven) Wert besitzt. Läßt man nun $u_1, u_2 \cdots u_{\nu-1}$ alle ganzen rationalen Zahlen durchlaufen, so erhält man eine **Gruppe** R' von unendlich vielen in $\mathfrak{o}'$ enthaltenen Einheiten

$$\varrho_1'^{u_1} \varrho_2'^{u_2} \cdots \varrho_{\nu-1}'^{u_{\nu-1}},$$

die sich durch Multiplikation und Division reproduzieren; je zwei verschiedenen Systemen von Exponenten entsprechen zwei verschiedene Individuen der Gruppe R'. Die Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$, welche eine **Basis** der Gruppe R' bilden, können offenbar ohne Änderung von R' und $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ durch je $(\nu - 1)$ Einheiten ersetzt werden, welche aus R' so ausgewählt sind, daß die aus den zugehörigen $(\nu - 1)^2$ Exponenten u gebildete Determinante $= 1$ wird. Bezeichnet man mit $R'\alpha$ den Inbegriff aller Produkte aus einer bestimmten Zahl α und jeder der in R' enthaltenen Einheiten, so sind zwei solche Komplexe entweder gänzlich identisch, oder sie haben keine einzige Zahl gemeinschaftlich; das System **aller** Einheiten ε' der Ordnung $\mathfrak{o}'$ besteht (D. § 166, 6.) aus einer **endlichen**, von R' abhängigen Anzahl r' solcher Komplexe, woraus leicht folgt, daß $\varepsilon'^{r'}$ stets der Gruppe R' angehört. Hieraus ergibt sich unmittelbar, daß unter allen Systemen von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ auch solche Systeme $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ existieren, für welche die Determinante $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ einen **Minimumwert** erhält; dann besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus r' Komplexen von der Form

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1},$$

wo ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$ bedeutet (D. § 166, 7.). Ein solches System von $(\nu - 1)$ unabhängigen Einheiten $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ heißt ein Fundamental-System der Ordnung $\mathfrak{o}'$, und wir wollen zur Abkürzung den durch die Ordnung $\mathfrak{o}'$ vollständig bestimmten Quotienten

$$\frac{L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})}{r'} = \mathrm{E}(\mathfrak{o}')$$

setzen*). Es würde sich, wie wir beiläufig bemerken, durch Betrachtungen, welche den gleich folgenden sehr ähnlich sind (vgl. D. § 161), auch leicht beweisen lassen, daß Zähler und Nenner dieses Quotienten sich mit einer und derselben ganzen rationalen Zahl multiplizieren, wenn das Fundamental-System $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ durch ein beliebiges System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ ersetzt wird. Wir wollen nun beweisen, daß die in dem Verhältnis $h' : h = m$ auftretende Anzahl s der Komplexe $\varepsilon' \varepsilon_1$, $\varepsilon' \varepsilon_2 \cdots \varepsilon' \varepsilon_s$, aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht,

$$= \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})}$$

ist.

Zu diesem Zwecke bezeichnen wir mit $\varrho_1, \varrho_2 \cdots \varrho_{\nu-1}$ ein Fundamental-System von Einheiten der Ordnung $\mathfrak{o}$, mit R die zugehörige Gruppe der aus ihnen durch Multiplikation und Division gebildeten Einheiten, und mit r die Anzahl der Komplexe

$$R, R\varrho, R\varrho^2 \cdots R\varrho^{r-1},$$

aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht, wo nun ϱ eine primitive Wurzel der Gleichung $\varrho^r = 1$ bedeutet. Unter diesen Einheiten ε befinden sich auch alle Einheiten ε' der Ordnung $\mathfrak{o}'$, weil $\mathfrak{o}'$ durch $\mathfrak{o}$ teilbar ist. Ist nun e ein bestimmter Index aus der Reihe 0, 1, 2 $\cdots (\nu - 1)$, so gibt es unter allen denjenigen Einheiten von der Form

$$\sigma'_e = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_e^{u_e},$$

welche, wie z. B. ϱ_e^s, auch der Ordnung $\mathfrak{o}'$ angehören, mindestens eine

$$\varrho'_e = \varrho^{a^{(e)}} \varrho_1^{a_1^{(e)}} \varrho_2^{a_2^{(e)}} \cdots \varrho_e^{a_e^{(e)}},$$

*) In dem singulären Falle eines imaginären quadratischen Körpers ($n = 2$, $\nu = 1$) besteht R' aus der einzigen Einheit 1, r' bedeutet die endliche Anzahl aller in $\mathfrak{o}'$ enthaltenen Einheiten, und die Determinante $L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})$ ist durch 1 zu ersetzen.

in welcher der letzte Exponent u_e seinen kleinsten positiven Wert $a_e^{(e)}$ erreicht, und es leuchtet ein, daß in jeder anderen Einheit σ_e' der letzte Exponent u_e notwendig durch $a_e^{(e)}$ teilbar, also von der Form $a_e^{(e)} x_e$ sein muß, wo x_e eine ganze rationale Zahl bedeutet; es wird daher

$$\sigma_e' \varrho_e'^{-x_e}$$

eine in $\mathfrak{o}'$ enthaltene Einheit von der Form σ_{e-1}', oder $= 1$ sein, wenn $e = 0$ ist. In diesem letzteren Falle ist

$$\varrho' = \varrho^a,$$

und da $\varrho^r = 1$ eine Einheit der Ordnung $\mathfrak{o}'$ ist, so muß r durch a teilbar, also

$$r = ar'$$

sein, und folglich ist ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$. Hat man nun nach der obigen Vorschrift für jeden Index $e = 0, 1, 2 \cdots (\nu - 1)$ eine solche partikuläre Einheit ϱ', ϱ_1', $\varrho_2' \cdots \varrho_{\nu-1}'$ der Ordnung $\mathfrak{o}'$ aufgestellt, so ergibt sich, daß jede Einheit ε' der Ordnung $\mathfrak{o}'$, d. h. jede Einheit $\sigma_{\nu-1}'$, von der Form

$$\sigma_{\nu-2}' \varrho_{\nu-1}'^{x_{\nu-1}} = \sigma_{\nu-3}' \varrho_{\nu-2}'^{x_{\nu-2}} \varrho_{\nu-1}'^{x_{\nu-1}} = \text{usw.},$$

also schließlich von der Form

$$\varepsilon' = \varrho'^{x} \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}}$$

ist, wo $x, x_1, x_2 \cdots x_{\nu-1}$ ganze rationale Zahlen bedeuten, deren erste x auf die r' Werte $0, 1, 2 \cdots (r' - 1)$ einzuschränken ist; umgekehrt leuchtet ein, daß alle Zahlen ε' von der vorstehenden Form auch wirklich Einheiten der Ordnung $\mathfrak{o}'$ sind. Da die Zahlen $a, a_1', a_2'' \cdots a_{\nu-1}^{(\nu-1)}$ sämtlich positiv sind, so ist auch ihr Produkt

$$A = a a_1' a_2'' \cdots a_{\nu-1}^{(\nu-1)}$$

positiv; nun ergibt sich aus der Bildung der Einheiten $\varrho_1', \varrho_2'' \cdots \varrho_{\nu-1}'$, daß

$$L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}') = \frac{A}{a} L(\varrho_1, \varrho_2 \cdots \varrho_{\nu-1})$$

einen von 0 verschiedenen, positiven Wert hat; mithin bilden dieselben ein System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$, ja sogar ein Fundamental-System, weil für jedes beliebige System von $(\nu - 1)$ Einheiten $\varepsilon_1', \varepsilon_2' \cdots \varepsilon_{\nu-1}'$ dieser Ordnung $\mathfrak{o}'$ offenbar $L(\varepsilon_1', \varepsilon_2' \cdots \varepsilon_{\nu-1}') = pL(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ wird, wo p eine ganze rationale Zahl bedeutet. Bezeichnet man wieder mit R' die Gruppe aller Einheiten, welche

aus $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ durch Multiplikation und Division gebildet werden können, so besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus den r' verschiedenen Komplexen

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1}.$$

Da ferner oben $r = ar'$ gefunden ist, so ergibt sich aus der vorhergehenden Gleichung

$$\mathrm{E}(\mathfrak{o}') = A\,\mathrm{E}(\mathfrak{o}).$$

Nun ist offenbar A die Anzahl aller derjenigen in $\mathfrak{o}$ enthaltenen Einheiten

$$\varepsilon_0 = \varrho^v \varrho_1^{v_1} \varrho_2^{v_2} \cdots \varrho_{\nu-1}^{v_{\nu-1}},$$

deren Exponenten den Bedingungen

$$0 \leqq v < a, \quad 0 \leqq v_1 < a_1' \cdots 0 \leqq v_{\nu-1} < a_{\nu-1}^{(\nu-1)}$$

genügen. Da ferner jede Einheit der Ordnung $\mathfrak{o}'$ die Form

$$\varepsilon' = \varrho'^x \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}} = \varrho^w \varrho_1^{w_1} \varrho_2^{w_2} \cdots \varrho_{\nu-1}^{w_{\nu-1}}$$

hat, wo

$$\begin{aligned}
w_{\nu-1} &= a_{\nu-1}^{(\nu-1)} x_{\nu-1} \\
w_{\nu-2} &= a_{\nu-2}^{(\nu-1)} x_{\nu-1} + a_{\nu-2}^{(\nu-2)} x_{\nu-2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
w_1 &= a_1^{(\nu-1)} x_{\nu-1} + a_1^{(\nu-2)} x_{\nu-2} + \cdots + a_1' x_1 \\
w &= a^{(\nu-1)} x_{\nu-1} + a^{(\nu-2)} x_{\nu-2} + \cdots + a' x_1 + a x
\end{aligned}$$

ist, so kann man, wenn eine beliebige Einheit

$$\varepsilon = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_{\nu-1}^{u_{\nu-1}}$$

der Ordnung $\mathfrak{o}$ gegeben ist, die Einheit ε', d. h. die Exponenten $x_{\nu-1}, x_{\nu-2} \cdots x_1, x$ stets und nur auf einzige Weise so wählen, daß die Zahlen

$$v = u - w, \quad v_1 = u_1 - w_1 \cdots v_{\nu-1} = u_{\nu-1} - w_{\nu-1}$$

den obigen Bedingungen genügen, daß also $\varepsilon\varepsilon'^{-1}$ eine der A Einheiten ε_0 wird; jede Einheit ε der Ordnung $\mathfrak{o}$ läßt sich daher stets und nur auf eine einzige Weise in die Form $\varepsilon'\varepsilon_0$ setzen, wo ε' eine Einheit in $\mathfrak{o}'$, ε_0 eine der obigen A Einheiten in $\mathfrak{o}$ bedeutet. Durchläuft ε' alle Einheiten der Ordnung $\mathfrak{o}'$, während ε_0 konstant bleibt, so erhält man einen Komplex von unendlich vielen Einheiten $\varepsilon = \varepsilon'\varepsilon_0$, und zwei solche Komplexe, welche zwei verschiedenen Werten von ε_0 entsprechen, sind gänzlich verschieden voneinander; mithin besteht

das System aller Einheiten ε der Ordnung $\mathfrak{o}$ aus A solchen Komplexen. Aber es ist oben gezeigt, daß die Anzahl dieser Komplexe $= s$ ist; mithin ist $s = A$, d. h.

$$s = \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})},$$

was zu beweisen war.

Hiernach nimmt das frühere Resultat für das Verhältnis der Klassenanzahlen die folgende Form an

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{k})}{\psi'(\mathfrak{k})} \cdot \frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')},$$

in welcher die Lösung unseres Problems nach der Methode von Gauß enthalten ist.

§ 11.

Zerlegbare Formen, welche den Idealen von beliebiger Ordnung entsprechen.

Bevor wir zu der Ableitung desselben Resultates nach der Methode von Dirichlet übergehen, wird es zweckmäßig sein, mit einigen Worten den Zusammenhang zwischen den Idealen von beliebiger Ordnung und den zerlegbaren Formen des Körpers Ω zu besprechen.

Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine bestimmte Basis der aus allen ganzen Zahlen des Körpers bestehenden Ordnung $\mathfrak{o}$, so wollen wir die n Basiszahlen

$$\omega_i' = k_1^{(i)}\omega_1 + k_2^{(i)}\omega_2 + \cdots + k_n^{(i)}\omega_n$$

der Ordnung $\mathfrak{o}'$ (§ 3) und die n Basiszahlen

$$\alpha_i' = a_1^{(i)}\omega_1' + a_2^{(i)}\omega_2' + \cdots + a_n^{(i)}\omega_n'$$

eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ (§ 4) immer so wählen, daß die Determinanten

$$\sum \pm k_1' k_2'' \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k,$$
$$\sum \pm a_1' a_2'' \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}') = N'(\mathfrak{a}')$$

werden, also positive Werte erhalten.

Die sämtlichen Zahlen des Ideals $\mathfrak{a}'$ sind von der Form

$$\alpha' = x_1\alpha_1' + x_2\alpha_2' + \cdots + x_n\alpha_n',$$

wo die Variablen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, und es ergibt sich, genau wie für die Ideale in $\mathfrak{o}$ (D. § 165), daß

$$N(\alpha') = N'(\mathfrak{a}')X$$

ist, wo X eine homogene Funktion n-ten Grades der n Variablen $x_1, x_2 \cdots x_n$ mit ganzen rationalen Koeffizienten bedeutet, welche, wie aus § 6 folgt, keinen gemeinschaftlichen Teiler haben; die Determinante dieser Form X (§ 1) ist

$$= D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2,$$

wo $D = \Delta(\Omega)$ wieder die Grundzahl des Körpers Ω bedeutet. Alle Formen X, welche allen verschiedenen Basen aller mit $\mathfrak{a}'$ äquivalenten Ideale entsprechen, sind äquivalent, d. h. sie gehen durch lineare Substitutionen mit ganzen rationalen Koeffizienten, deren Determinanten $= +1$ sind, ineinander über; jeder Idealklasse entspricht also eine bestimmte Formenklasse. Der Multiplikation zweier Ideale $\mathfrak{a}'$, $\mathfrak{b}''$ der Ordnungen $\mathfrak{o}'$, $\mathfrak{o}''$ oder der Komposition der sie enthaltenden Idealklassen A', B'' entspricht die Komposition der zu den Idealen $\mathfrak{a}'\,\mathfrak{b}''$ gehörigen Formen X, Y zu einer dem Ideal $\mathfrak{a}'\,\mathfrak{b}''$ entsprechenden Form Z, deren Determinante

$$= D(\mathfrak{o}, \mathfrak{o}'\,\mathfrak{o}'')^2$$

ist, und zugleich folgt hieraus die Komposition der Formenklassen*).

Um die Rückkehr von diesen allgemeinen Untersuchungen zu dem Falle der quadratischen Körper und Formen zu erleichtern, füge ich noch folgende Bemerkungen hinzu, von deren Richtigkeit man sich leicht überzeugen wird (vgl. D. §§ 168 bis 170). Jede Wurzel einer irreduktiblen quadratischen Gleichung ist von der Form $a + b\sqrt{c}$, wo c eine ganze rationale Zahl bedeutet, welche keine Quadratzahl und auch durch keine Quadratzahl außer 1 teilbar ist; a und b sind rationale Zahlen, und b ist von 0 verschieden. Die Grundzahl D des quadratischen Körpers Ω, welcher aus der Zahl $a + b\sqrt{c}$ entspringt, ist $= c$ oder $= 4c$, je nachdem $c \equiv 1$, oder $c \equiv 2, 3 \pmod 4$ ist; setzt man

$$\Theta = \frac{D + \sqrt{D}}{2},$$

so bilden die Zahlen 1, Θ eine Basis der Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen

$$\omega = \frac{t + u\sqrt{D}}{2}$$

*) Da, wie schon oben (§ 7, Anmerkung) bemerkt ist, Moduln existieren, welche keinem Ideal äquivalent sind, so ist, was ich hervorheben zu müssen glaube, in dem Obigen noch nicht die Theorie aller zerlegbaren Formen enthalten, welche den sämtlichen Moduln eines Körpers Ω entsprechen.

des Körpers besteht, wo t, u alle, der Bedingung $t \equiv Du \pmod 2$ genügenden Paare von ganzen rationalen Zahlen zu durchlaufen haben. Jede Ordnung $\mathfrak{o}'$ ist dann von der Form $[1, k\Theta]$, wo $k = (\mathfrak{o}, \mathfrak{o}')$ eine beliebige positive ganze rationale Zahl bedeutet; der Führer k einer solchen Ordnung ist das Hauptideal $\mathfrak{o}k = [k, k\Theta]$, und es ist $N(\mathfrak{k}) = k^2$. Setzt man, wenn p eine positive rationale Primzahl bedeutet,

$$(D, p) = 0, \ +1 \text{ oder } -1,$$

je nachdem $\mathfrak{o}p$ das Quadrat eines Primideals, das Produkt aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist (vgl. D. § 168), so ist

$$\psi(\mathfrak{o}k) = k^2 \prod \left(1 - \frac{1}{p}\right)\left(1 - \frac{(D, p)}{p}\right),$$

wo p alle verschiedenen in k aufgehenden Primzahlen durchläuft; da ferner jede Zahl der Ordnung $\mathfrak{o}'$ mit einer rationalen Zahl kongruent ist in bezug auf $\mathfrak{o}k$, so ist

$$\psi'(\mathfrak{o}k) = \varphi(k) = k \prod \left(1 - \frac{1}{p}\right),$$

und folglich

$$\frac{\psi(\mathfrak{o}k)}{\psi'(\mathfrak{o}k)} = k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Ist nun der Körper Ω imaginär, also D negativ, so ist (vgl. § 10 Anmerkung)

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{r'}{r},$$

wo r die Anzahl aller Einheiten in $\mathfrak{o}$, und r' die Anzahl aller Einheiten in $\mathfrak{o}'$ bedeutet. Die letztere Anzahl r' ist (wenn $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist) immer $= 2$, und ebenso ist r immer $= 2$, ausgenommen die beiden Fälle $D = -3$, wo $r = 6$, und $D = -4$, wo $r = 4$ ist. Es ist daher im allgemeinen

$$\frac{h'}{h} = m = k \prod \left(1 - \frac{(D, p)}{p}\right),$$

aber dieses Produkt ist im Falle $D = -3$ durch 3, im Falle $D = -4$ durch 2 zu dividieren. Ist der Körper Ω reell, also D positiv, so ist $r = r' = 2$, und folglich

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{\log \varepsilon}{\log \varepsilon'},$$

wo, wenn $k\sqrt{D} = \sqrt{D'}$ gesetzt wird,

$$\varepsilon = \frac{T + U\sqrt{D}}{2}, \quad \varepsilon' = \frac{T' + U'\sqrt{D'}}{2}$$

die Fundamentaleinheiten der Ordnungen o, o' bedeuten, und man erhält

$$\frac{h'}{h} = \frac{\log \varepsilon}{\log \varepsilon'} \cdot k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Was das Zeichen (D, p) betrifft, so ist sein Wert $= 0$, wenn p in D aufgeht; ist $p = 2$ und D ungerade, also $D \equiv 1 \pmod 4$, so ist $(D, p) = +1$ oder $= -1$, je nachdem $D \equiv 1 \pmod 8$ oder $D \equiv 5 \pmod 8$; ist endlich p ungerade, und D nicht teilbar durch p, so ist unter Anwendung der Bezeichnung von Legendre

$$(D, p) = \left(\frac{D}{p}\right).$$

Jeder Idealklasse in o' entspricht nach den obigen Festsetzungen eine Klasse von äquivalenten quadratischen Formen $ax^2 + bxy + cy^2$, deren konstante Koeffizienten a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Teiler sind, und die gemeinschaftliche Determinante*) dieser Formen ist $D' = b^2 - 4ac = Dk^2$; wenn D negativ ist, so treten nur sogenannte positive, d. h. solche Formen auf, deren äußere Koeffizienten a, c positiv sind. Umgekehrt entspricht eine bestimmte Klasse von äquivalenten quadratischen Formen, deren Determinante D' keine Quadratzahl ist, immer einer und nur einer Idealklasse eines quadratischen Körpers Ω, und wenn o' die Ordnung dieser Idealklasse bedeutet, so ist $D' = D(o, o')^2 = Dk^2$, wo D die Grundzahl von Ω ist. Mithin sind in den obigen Formeln die verschiedenen Sätze enthalten, welche sich auf die Anzahl der quadratischen Formen in verschiedenen Ordnungen und auf die Unterscheidung der eigentlich und uneigentlich primitiven Formen beziehen.

§ 12.

Methode von Dirichlet.

Wir wenden uns nun der zweiten Lösung desselben allgemeinen Problems zu, welche auf den von Dirichlet eingeführten Prinzipien

*) Es ist wohl darauf zu achten, daß die hier im Sinne von § 1 definierte Determinante das Vierfache der Zahl ist, welche von Gauß die Determinante der Form genannt wird, während der Begriff der (eigentlichen) Äquivalenz der Formen derselbe bleibt.

beruht. Durchläuft $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so konvergiert die Reihe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s}$$

für alle positiven Werte von $(s-1)$; denn weil $N'(\mathfrak{a}') = N(\mathfrak{o}\,\mathfrak{a}')$ ist (§ 5, 1°), so bilden die Glieder dieser Reihe nur einen Teil der gleichfalls aus lauter positiven Gliedern bestehenden Reihe

$$S = \sum \frac{s-1}{N(\mathfrak{a})^s},$$

in welcher $\mathfrak{a}$ alle Ideale der Ordnung $\mathfrak{o}$ durchläuft, und deren Konvergenz schon früher bewiesen ist (D. § 167); übrigens ergibt sich die Konvergenz der Reihe S' auch aus den weiter unten folgenden Untersuchungen.

Unsere Hauptaufgabe besteht darin, den Grenzwert zu ermitteln, welchem die Summe S' sich für unendlich kleine positive Werte von $(s-1)$ annähert. Zu diesem Zwecke betrachten wir aber zunächst nur denjenigen Teil S'' der Reihe S', welcher allen, durch ein gegebenes Ideal $\mathfrak{m}'$ der Ordnung $\mathfrak{o}'$ teilbaren Hauptidealen $\mathfrak{a}'$ entspricht. Die allgemeine Form dieser Ideale $\mathfrak{a}'$ ergibt sich auf die folgende Weise.

1. Jedes Ideal $\mathfrak{a}'$ ist von der Form $\mu\,\mathfrak{o}'$, wo μ eine in $\mathfrak{o}'$ enthaltene Zahl bedeutet, welche relative Primzahl zu dem Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist.

2. Die Zahl μ muß in dem gegebenen Ideal $\mathfrak{m}'$ enthalten sein.

3. Die Norm der Zahl μ muß positiv sein.

Umgekehrt, wenn μ diese drei Bedingungen erfüllt, so ist $\mu\,\mathfrak{o}'$ jedenfalls eins von den Idealen $\mathfrak{a}'$, auf welche sich die Summe S'' erstreckt.

Bilden nun die Zahlen $\mu_1, \mu_2 \cdots \mu_n$ eine Basis des gegebenen Ideals $\mathfrak{m}'$, so ist zur Erfüllung der Bedingung 2 erforderlich und hinreichend, daß

$$\mu = m_1\mu_1 + m_2\mu_2 + \cdots + m_n\mu_n$$

sei, wo $m_1, m_2 \cdots m_n$ ganze rationale Zahlen bedeuten, und da $\mathfrak{m}'$ durch $\mathfrak{o}'$ teilbar ist, so ist jede solche Zahl μ auch in $\mathfrak{o}'$ enthalten. Aber sie soll zufolge 1. auch relative Primzahl zu $\mathfrak{f}$ sein. Bezeichnen wir nun wieder (wie in § 9) mit $\psi'(\mathfrak{f})$ die Anzahl aller in $\mathfrak{o}'$ ent-

haltenen Zahlen ω', welche inkongruent in bezug auf $\mathfrak{k}$ und zugleich relative Primzahlen zu $\mathfrak{k}$ sind, so muß gleichzeitig

$$\mu \equiv \omega' \pmod{\mathfrak{k}}, \quad \mu \equiv 0 \pmod{\mathfrak{m}'}$$

sein; da $\mathfrak{k} + \mathfrak{m}' = \mathfrak{o}'$ ist, so gibt es (nach § 2, 2°) immer Zahlen μ, welche einem solchen Kongruenzpaar genügen, und sie bilden eine bestimmte Zahlklasse in bezug auf den Modul $\mathfrak{k} - \mathfrak{m}'$, welcher offenbar $= \mathfrak{k}\mathfrak{m}'$ ist; denn da $\mathfrak{m}' > \mathfrak{o}\mathfrak{m}'$ ist, so ist $\mathfrak{k} - \mathfrak{m}'$ ein gemeinschaftliches Vielfaches der beiden relativen Primideale $\mathfrak{k}, \mathfrak{o}\mathfrak{m}'$, also auch ein Vielfaches ihres Produkts $\mathfrak{k}\mathfrak{o}\mathfrak{m}' = \mathfrak{k}\mathfrak{m}'$, und umgekehrt ist $\mathfrak{k}\mathfrak{m}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{k}$ und $\mathfrak{m}'$, weil $\mathfrak{m}' > \mathfrak{o}$, $\mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{o} = \mathfrak{k}$, $\mathfrak{o}'\mathfrak{m}' = \mathfrak{m}'$ ist. Die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, bilden daher $\psi'(\mathfrak{k})$ verschiedene Zahlklassen (mod. $\mathfrak{k}\mathfrak{m}'$). Jede solche Zahlklasse besteht aber, weil $k\mathfrak{m}' > \mathfrak{k}\mathfrak{m}''$ ist, aus $(\mathfrak{k}\mathfrak{m}, k\mathfrak{m}')$ verschiedenen Zahlklassen (mod. $k\mathfrak{m}'$), und folglich ist

$$c = \psi'(\mathfrak{k})\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}')$$

die Anzahl der Zahlklassen (mod. $k\mathfrak{m}'$), aus welchen das System aller dieser Zahlen μ besteht. Es läßt sich leicht zeigen, daß diese Anzahl c von $\mathfrak{m}'$ unabhängig ist. In der Tat, aus

$$(\mathfrak{o}, \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}')\,(\mathfrak{o}', \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}')$$

folgt

$$k N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}'),$$

mithin, weil $N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')$ ist (§ 5, 1°), $(\mathfrak{o}\mathfrak{m}', \mathfrak{m}') = k$, also auch

$$(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = k,$$

weil offenbar für je zwei Moduln $\mathfrak{a}, \mathfrak{b}$ der Satz $(\eta\mathfrak{a}, \eta\mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ gilt, sobald η eine von 0 verschiedene Zahl ist. Da ferner

$$(\mathfrak{o}, k\mathfrak{o}\mathfrak{m}') = (\mathfrak{o}, \mathfrak{k}\mathfrak{m}')\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}'),$$

also

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}') = \frac{N(k\mathfrak{o}\mathfrak{m}')}{N(\mathfrak{k}\mathfrak{m}')} = \frac{N(k\mathfrak{o})}{N(\mathfrak{k})} = \frac{k^n}{N(\mathfrak{k})}$$

ist, so ergibt sich

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}') = (\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}')\,(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = \frac{k^{n+1}}{N(\mathfrak{k})},$$

und folglich ist

$$c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})}\, k^{n+1}$$

die Anzahl der fraglichen Zahlklassen in bezug auf den Modul

$$k\mathfrak{m}' = [k\mu_1, k\mu_2 \cdots k\mu_n].$$

Wählt man aus jeder dieser Klassen einen bestimmten Repräsentanten

$$a_1\mu_1 + a_2\mu_2 + \cdots + a_n\mu_n,$$

so werden alle Zahlen μ derselben Klasse durch die Form

(I) $$\mu = (a_1 + kz_1)\mu_1 + (a_2 + kz_2)\mu_2 + \cdots + (a_n + kz_n)\mu_n$$

erzeugt, wenn $z_1, z_2 \cdots z_n$ alle ganzen rationalen Zahlen durchlaufen; und die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, werden durch c solche lineare Formen erzeugt, und zwar jede nur einmal.

Von diesen Zahlen μ sind aber nur diejenigen beizubehalten, welche auch der dritten Bedingung

(II) $$N(\mu) > 0$$

genügen. Umgekehrt erzeugt jede solche Zahl μ ein Hauptideal $\mu\mathfrak{o}'$ in $\mathfrak{o}'$, welches durch das gegebene Ideal $\mathfrak{m}'$ teilbar ist.

Aber es leuchtet ein, daß, wenn μ **alle** diese Zahlen durchläuft, jedes bestimmte, durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}'$ unendlich oft erzeugt wird. Ist nämlich μ_0 eine bestimmte von diesen Zahlen μ, so wird dasselbe Hauptideal $\mathfrak{o}'\mu_0$ offenbar durch alle, und nur durch die Zahlen μ erzeugt, welche von der Form $\mu = \varepsilon'\mu_0$ sind, wo ε' eine beliebige in $\mathfrak{o}'$ enthaltene Einheit (von positiver Norm) bedeutet. Um dies zu vermeiden, muß man den Zahlen μ neue Beschränkungen auferlegen. Zu diesem Zwecke kehren wir zu den Betrachtungen und Bezeichnungen des § 10 zurück und erweitern die Bedeutung der dort erklärten ν Symbole $l', l'' \cdots l^{(\nu)}$. Ist $\omega = \varphi(\Theta)$ eine **beliebige** von 0 verschiedene Zahl des Körpers Ω, und $\omega' = \varphi(\Theta')$, so verstehen wir unter $l'(\omega)$ den reellen Teil des Logarithmen von

$$\frac{\omega'}{\sqrt[n]{N(\omega)}}$$

oder das Doppelte dieses reellen Teiles, je nachdem Θ' eine reelle oder imaginäre Wurzel der irreduktiblen Gleichung $f(\Theta') = 0$ ist; legt man ferner den Symbolen $l''(\omega), l'''(\omega) \cdots l^{(\nu)}(\omega)$ die entsprechende Bedeutung in bezug auf die Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ bei, so ist offenbar

$$l'(\omega) + l''(\omega) + \cdots + l^{(\nu)}(\omega) = 0.$$

Bilden nun $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ ein bestimmtes Fundamentalsystem $\mathfrak{R}$ von Einheiten der Ordnung $\mathfrak{o}'$, so wollen wir unter den **Exponenten**

der Zahl ω in bezug auf $\mathfrak{R}$ diejenigen völlig bestimmten reellen Werte $x_1(\omega)$, $x_2(\omega) \cdots x_{\nu-1}(\omega)$ verstehen, welche den ν Gleichungen

$$\begin{aligned} l'(\varrho_1')\,x_1(\omega) + l'(\varrho_2')\,x_2(\omega) + \cdots + l'(\varrho_{\nu-1}')\,x_{\nu-1}(\omega) &= l'(\omega) \\ l''(\varrho_1')\,x_1(\omega) + l''(\varrho_2')\,x_2(\omega) + \cdots + l''(\varrho_{\nu-1}')\,x_{\nu-1}(\omega) &= l''(\omega) \\ \cdots\cdots\cdots\

Nun zerlegen wir diese Summe abermals in c Partialsummen, indem wir jedesmal die Beiträge derjenigen Zahlen μ zu einer Partialsumme sammeln, welche in einer und derselben Linearform (I) enthalten sind und außerdem den Bedingungen (II) und (III) genügen. Es sei t eine beliebige positive Größe, und T die entsprechende Anzahl dieser Zahlen μ, für welche zugleich

$$N(\mu) \leqq t \tag{IV}$$

wird, so wollen wir beweisen, daß der Quotient $T:t$ mit unendlich wachsendem t sich einem endlichen Grenzwerte nähert. Zu diesem Zwecke bezeichnen wir mit

$$h_1, h_2 \cdots h_n$$

ein System von reellen, stetig veränderlichen Größen und betrachten die n homogenen linearen Funktionen $\omega', \omega'' \cdots \omega^{(n)}$, welche aus

$$\omega = h_1\mu_1 + h_2\mu_2 + \cdots + h_n\mu_n$$

dadurch hervorgehen, daß die dem Körper Ω angehörigen Konstanten $\mu_1, \mu_2 \cdots \mu_n$ durch die mit ihnen konjugierten Zahlen ersetzt werden, welche der Reihe nach den Wurzeln $\Theta', \Theta'' \cdots \Theta^{(n)}$ der Gleichung $f(\Theta) = 0$ entsprechen. Setzen wir auch in allen Fällen, wo die Werte der Variablen $h_1, h_2 \cdots h_n$ nicht sämtlich rational sind, der Kürze wegen

$$\omega'\omega'' \cdots \omega^{(n)} = N(\omega),$$

so ist $N(\omega)$ eine homogene Funktion n-ten Grades von den Variabeln $h_1, h_2 \cdots h_n$. Wir beschränken nun zunächst die Variabilität dieser Größen durch die Bedingung

$$0 < N(\omega) \leqq 1 \tag{V}$$

und definieren hierauf ein System von ν Funktionen

$$l'(\omega), l''(\omega) \cdots l^{(\nu)}(\omega)$$

und aus diesem ein System von $(\nu - 1)$ Funktionen

$$x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$$

genau nach denselben Regeln, wie dies oben für den Fall geschehen ist, daß die sämtlichen Variablen $h_1, h_2 \cdots h_n$ rationale Werte haben, und folglich ω eine Zahl des Körpers Ω ist. Hierauf beschränken

wir die Variabilität der Größen $h_1, h_2 \cdots h_n$ ferner durch die $(\nu - 1)$ Bedingungen

(VI) $$0 \leqq x_1(\omega) < 1 \cdots 0 \leqq x_{\nu-1}(\omega) < 1.$$

Hierdurch, sowie durch die Bedingung (V), ist den Variablen $h_1, h_2 \cdots h_n$ ein bestimmtes Gebiet G angewiesen, und zwar ist (vgl. D. § 167) das über dieses Gebiet G ausgedehnte n-fache Integral

$$g = \int dh_1\, dh_2 \cdots dh_n = \frac{\sigma L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')}{\sqrt{\pm \Delta(\mu_1, \mu_2 \cdots \mu_n)}} = \frac{\sigma r' \mathrm{E}(o')}{kN'(\mathfrak{m}')\sqrt{\pm D}},$$

wo $\sigma = 2^{\nu-1}\pi^{n-\nu}$, im Falle $n = 2\nu$ aber $= (2\pi)^\nu$ ist; $\sqrt{\pm D}$ bedeutet die positive Quadratwurzel aus dem absoluten Werte der Grundzahl D des Körpers Ω.

Die oben mit T' bezeichnete Anzahl der in einer bestimmten Linearform (I) erhaltenen Zahlen μ, welche außerdem den Bedingungen (II), (III), (IV) genügen, besitzt nun die folgende Bedeutung für das eben definierte Gebiet G. Setzt man

$$h_1 = \frac{a_1 + kz_1}{\sqrt[n]{t}}, \quad h_2 = \frac{a_2 + kz_2}{\sqrt[n]{t}} \cdots h_n = \frac{a_n + kz_n}{\sqrt[n]{t}},$$

so bringt jedes System von n ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$, welchem eine solche Zahl μ entspricht, ein System von n reellen Werten $h_1, h_2 \cdots h_n$ hervor, welches dem Gebiete G angehört; denn da $N(\omega)$ eine homogene Funktion n-ten Grades, jede der Funktionen $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ aber eine homogene Funktion 0-ten Grades von den Variablen $h_1, h_2 \cdots h_n$ ist, so gehen die Bedingungen (II) und (IV) in die Bedingung (V), und die Bedingungen (III) in die Bedingungen (VI) über. Setzt man ferner

$$\frac{k}{\sqrt[n]{t}} = \delta; \quad \frac{a_1}{\sqrt[n]{t}} = h_1^0, \quad \frac{a_2}{\sqrt[n]{t}} = h_2^0 \cdots \frac{a_n}{\sqrt[n]{t}} = h_n^0,$$

so ist das durch $z_1, z_2 \cdots z_n$ hervorgebrachte, dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$ von der Beschaffenheit, daß die Größen

$$\frac{h_1 - h_1^0}{\delta} = z_1, \quad \frac{h_2 - h_2^0}{\delta} = z_2 \cdots \frac{h_n - h_n^0}{\delta} = z_n$$

ganze rationale Zahlen werden; und umgekehrt leuchtet ein, daß jedes dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$, welches dieser letzten Bedingung genügt, rückwärts ein System von ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$ und dadurch eine Zahl μ der Linearform (I) hervorbringt, welche auch den Bedingungen (II), (III), (IV) genügt. Mithin ist T die Anzahl derjenigen dem Gebiet G angehörenden Wertsysteme $h_1, h_2 \cdots h_n$, für welche die Quotienten

$$\frac{h_1 - h_1^0}{\delta}, \frac{h_2 - h_2^0}{\delta} \cdots \frac{h_n - h_n^0}{\delta}$$

ganze rationale Zahlen werden. Wächst nun t über alle Grenzen, so wird δ unendlich klein, und aus dem Begriffe eines n-fachen bestimmten Integrals ergibt sich, daß

$$\lim (T\delta^n) = k^n \lim \left(\frac{T}{t}\right) = \int dh_1\, dh_2 \cdots dh_n = g$$

ist, mögen die Größen $h_1^0, h_2^0 \cdots h_n^0$ von δ unabhängig sein oder nicht. Nach einem Fundamentalsatze von Dirichlet (D. § 118) folgt hieraus, daß die auf alle Zahlen μ der einen Linearform (I) ausgedehnte Partialsumme

$$\frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}$$

für alle positiven Werte von $(s-1)$ konvergiert und für unendlich kleine Werte von $(s-1)$ sich dem Grenzwerte

$$\frac{1}{r'} \lim \left(\frac{T}{t}\right) = \frac{g}{k^n r'} = \frac{\sigma \mathrm{E}(\mathfrak{o}')}{k^{n+1} N(\mathfrak{m}') \sqrt{\pm D}}$$

nähert. Da derselbe von den Zahlen $a_1, a_2 \cdots a_n$, welche diese eine Linearform charakterisieren, gänzlich unabhängig ist, und da die Anzahl der Partialsummen, aus welchen die bis jetzt von uns betrachtete Summe S'' besteht,

$$= c = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} k^{n+1}$$

ist, so erhalten wir das Resultat

$$\lim S'' = \lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{N'(\mathfrak{m}') \sqrt{\pm D}},$$

wo links die Summe über alle durch $\mathfrak{m}'$ teilbaren Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnt ist.

§ 13.

Resultat dieser Methode.

Mit Hilfe des eben bewiesenen Satzes ist es leicht, unsere Aufgabe zu lösen. Nimmt man $\mathfrak{m}' = \mathfrak{o}'$, also $N'(\mathfrak{m}') = 1$, so ergibt sich

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

wo die Summe links über alle Ideale $\mathfrak{a}'$ ausgedehnt ist, welche der Hauptklasse O' der Ordnung $\mathfrak{o}'$ angehören.

Nun sei B' eine beliebige Ideal-Klasse der Ordnung $\mathfrak{o}'$, und $\mathfrak{m}'$ ein bestimmtes Ideal der inversen Klasse B'^{-1}. Durchläuft $\mathfrak{b}'$ alle Ideale der Klasse B', während $\mathfrak{m}'$ unverändert bleibt, so werden die Produkte $\mathfrak{b}'\mathfrak{m}'$ lauter Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$, welche durch $\mathfrak{m}'$ teilbar sind; und umgekehrt, ist $\mathfrak{a}'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal der Ordnung $\mathfrak{o}'$, so gibt es (nach § 5, 3°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{b}'\mathfrak{m}' = \mathfrak{a}'$ wird, und $\mathfrak{b}'$ muß notwendig der Klasse B' angehören, weil $\mathfrak{m}'$ ein Ideal der inversen Klasse ist. Da außerdem $N'(\mathfrak{b}'\mathfrak{m}') = N'(\mathfrak{b}')N'(\mathfrak{m}')$ ist, so ist die über alle Ideale $\mathfrak{b}'$ der Klasse B' ausgedehnte Summe

$$\sum \frac{s-1}{N'(\mathfrak{b}')^s} = N'(\mathfrak{m}')^s \sum \frac{s-1}{N'(\mathfrak{a}')^s},$$

wo $\mathfrak{a}'$ alle durch $\mathfrak{m}'$ teilbaren Hauptideale der Ordnung $\mathfrak{o}'$ durchläuft. Hieraus ergibt sich nach dem Schlußsatz des vorigen Paragraphen für unendlich kleine positive Werte von $(s-1)$

$$\lim \sum \frac{s-1}{N'(\mathfrak{b}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

d. h. der Grenzwert der über alle Ideale einer beliebigen Klasse in $\mathfrak{o}'$ ausgedehnten Summe ist für jede Klasse derselbe, und zwar offenbar von 0 verschieden.

Für den Spezialfall, in welchem $\mathfrak{o}'$ das Gebiet $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω ist, ergibt sich hieraus, weil

$$\mathfrak{f} = \mathfrak{o}, \quad N(\mathfrak{f}) = \psi'(\mathfrak{f}) = 1$$

wird, und weil die Anzahl h aller Ideal-Klassen der Ordnung $\mathfrak{o}$ endlich ist (D. § 164), das Resultat

$$\lim S = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = h \frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

wo die Summe über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ auszudehnen ist.

Durchläuft nun $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so durchläuft $\mathfrak{o}\mathfrak{a}'$ alle diejenigen Ideale der Ordnung $\mathfrak{o}$, welche relative Primideale zu dem Führer $\mathfrak{f}$ sind, und jedes nur ein einziges Mal. Da zugleich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$ ist, so ist die über alle Ideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnte Summe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \sum \frac{s-1}{N(\mathfrak{o}\mathfrak{a}')^s};$$

durchläuft aber $\mathfrak{p}$ alle verschiedenen in $\mathfrak{f}$ aufgehenden Primideale in $\mathfrak{o}$, so ist nach den allgemeinen Gesetzen der Teilbarkeit die über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ ausgedehnte Summe

$$\sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N(\mathfrak{o}\mathfrak{a}')^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N'(\mathfrak{a}')^s},$$

und folglich, weil

$$\prod \left(1-\frac{1}{N(\mathfrak{p})}\right) = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})}$$

ist,

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim \sum \frac{s-1}{N(\mathfrak{a})^s},$$

d. h.

$$\lim S' = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim S.$$

Da die rechte Seite einen endlichen Wert hat, so folgt zunächst, daß die Anzahl h' der Ideal-Klassen in $\mathfrak{o}'$ endlich sein muß, weil oben für jeden Bestandteil der linken Seite, welcher einer einzelnen Klasse entspricht, ein und derselbe von 0 verschiedene Grenzwert gefunden ist. Setzt man diesen Wert und ebenso den Grenzwert der rechten Seite ein, so ergibt sich

$$h' \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \cdot h \frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

und hieraus

$$\frac{h'}{h} = \frac{\psi(\mathfrak{f})}{\psi'(\mathfrak{f})} \cdot \frac{E(\mathfrak{o})}{E(\mathfrak{o}')},$$

was mit dem in § 10 nach der Methode von Gauß gefundenen Resultat übereinstimmt.

Erläuterungen zur vorstehenden Abhandlung.

Diese Abhandlung findet ihre Ergänzung in dem im Nachlaß veröffentlichten Überblick über die allgemeine Modultheorie (Brief an Frobenius von 1883); beides war — wie dort und an anderen Stellen ausgesprochen ist — gedacht als Grundlage für die allgemeinen Reziprozitätsgesetze.

In der Tat ist die in der Abhandlung behandelte Klasseneinteilung eine Strahlklasseneinteilung, wie sie der Klassenkörpertheorie zugrunde liegt, wenn auch noch nicht die allgemeinste. Der Ausdruck für das Verhältnis der Klassenanzahlen (§ 10, Schluß) findet sich genau in der allgemeingültigen Form; auch die gruppentheoretischen Beweismethoden sind ähnlich, wenn auch noch etwas komplizierter, als in der späteren allgemeinen Theorie (H. Weber, Math. Ann., Bd. 48, S. 433 ff.). In § 12 werden die transzendenten Methoden zum ersten Male auf solche allgemeineren Klasseneinteilungen übertragen, was später viel weitergehend von H. Weber im allgemeinsten Falle entwickelt wurde (Math. Ann., Bd. 49, S. 83 ff.). Auf Weber aber baut Takagi auf.

Idealtheoretisch liegt die Bedeutung der Abhandlung darin, daß zum ersten Male die Beziehung zwischen Idealen verschiedener Ringe vermöge Zuordnung von Durchschnitts- und Erweiterungsideal behandelt wird. Die hier entwickelten Begriffe lassen sich auf beliebige Ringe ausdehnen und führen zu einer Zuordnung von Klassen von Idealen im Unter- und Oberring, wobei wieder Durchschnitts-(Verengungs-)Ideal und Erweiterungsideal eine ausgezeichnete Rolle spielen (vgl. H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Ann., Bd. 97, 1927).

Noether.

XIII.

Erläuterungen zu zwei Fragmenten von Riemann.

[Bernhard Riemanns gesammelte mathematische Werke und wissenschaftlicher Nachlaß, 2. Aufl., S. 466—478 (1892)].

Die Entstehungszeit (September 1852) des ersten der beiden Fragmente[*)] macht es wahrscheinlich, daß Riemann darauf ausging, für die Abhandlung über die trigonometrischen Reihen[**)] Beispiele von Funktionen zu finden, die unendlich oft in jedem Intervall unstetig werden, und vielleicht sollte die zweite Untersuchung[***)], welche sich auf einem kaum leserlichen Blatte findet, demselben Zwecke dienen. Die hier von Riemann benutzte Methode zur Bestimmung des Verhaltens der in der Theorie der elliptischen Funktionen auftretenden Modulfunktionen für den Fall, daß das komplexe Periodenverhältnis

$$\omega = \frac{K'i}{K} = \frac{\log q}{\pi i} \tag{1}$$

sich einem rationalen Werte nähert, gestattet aber zugleich eine sehr interessante Anwendung auf die sogenannte Theorie der unendlich vielen Formen der ϑ-Funktionen, nämlich auf die Bestimmung der bei der Transformation erster Ordnung auftretenden Konstanten, welche bekanntlich von Jacobi und Hermite auf die Gaußschen Summen, also auf die Theorie der quadratischen Reste zurückgeführt ist. Die Darstellung dieses Zusammenhangs bildet den Gegenstand der folgenden Erläuterungen.

Den Mittelpunkt der Theorie dieser Modulfunktionen, welche man auch ganz unabhängig von der der elliptischen Funktionen aufstellen kann, und welche seit dem Erscheinen der ersten Auflage von Riemanns Werken der Gegenstand zahlreicher Untersuchungen geworden ist, bildet in gewissem Sinne die Funktion

$$\eta(\omega) = 1^{\frac{\omega}{24}} \Pi(1 - 1^{\omega\nu}) = q^{\frac{1}{12}} \Pi(1 - q^{2\nu}), \tag{2}$$

wo zur Abkürzung

$$e^{2\pi i z} = 1^z, \quad \text{also} \quad q = 1^{\frac{\omega}{2}} \tag{3}$$

[*) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 455—461.]
[**) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 227—264.]
[***) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 461—465.]

gesetzt ist, und wo das Produktzeichen sich auf alle natürlichen Zahlen ν erstreckt. Da diese Funktion der komplexen Variablen $\omega = x + yi$, deren Ordinate x stets positiv ist, im Innern des hierdurch begrenzten, einfach zusammenhängenden Gebietes nirgends Null oder unendlich groß wird, so sind auch alle Potenzen von $\eta(\omega)$ mit beliebigen Exponenten, und ebenso $log\,\eta(\omega)$ durchaus einwertige Funktionen von ω, sobald ihr Wert an einer bestimmten Stelle festgesetzt ist. Die Funktion $log\,\eta(\omega)$ soll dadurch definiert werden, daß, wenn y über alle Grenzen wächst, also q verschwindet, die Größe

$$log\,\eta(\omega) - \frac{\omega\pi i}{12} = 0 \tag{4}$$

wird; dann ist $log\,\eta(\omega)$ konjugiert mit $log\,\eta(-\omega')$, wo ω', wie immer im folgenden, die mit ω konjugierte Größe bedeutet. Nun ist bekanntlich (Fundam. nova § 36)

$$\eta(2\omega)\eta\left(\frac{\omega}{2}\right)\eta\left(\frac{1+\omega}{2}\right) = 1^{\frac{1}{48}}\eta(\omega)^3,$$

$$\sqrt[4]{k} = 1^{\frac{1}{48}}\sqrt{2}\,\frac{\eta(2\omega)}{\eta\left(\frac{1+\omega}{2}\right)},$$

$$\sqrt[4]{k'} = 1^{\frac{1}{48}}\frac{\eta\left(\frac{\omega}{2}\right)}{\eta\left(\frac{1+\omega}{2}\right)},$$

$$\sqrt{\frac{2K}{\pi}} = 1^{-\frac{1}{24}}\frac{\eta\left(\frac{1+\omega}{2}\right)^2}{\eta(\omega)},$$

also nach der obigen Festsetzung:

$$\begin{cases} log\,\eta(2\omega) + log\,\eta\left(\frac{\omega}{2}\right) + log\,\eta\left(\frac{1+\omega}{2}\right) = \frac{\pi i}{24} + 3\,log\,\eta(\omega), \\ log\,k = log\,4 + \frac{\pi i}{6} + 4\,log\,\eta(2\omega) - 4\,log\,\eta\left(\frac{1+\omega}{2}\right), \\ log\,k' = \frac{\pi i}{6} + 4\,log\,\eta\left(\frac{\omega}{2}\right) - 4\,log\,\eta\left(\frac{1+\omega}{2}\right), \\ log\,\frac{2K}{\pi} = -\frac{\pi i}{6} + 4\,log\,\eta\left(\frac{1+\omega}{2}\right) - 2\,log\,\eta(\omega), \end{cases} \tag{5}$$

wo die Logarithmen linker Hand (wie in den Fund. nova § 40) als einwertige Funktionen von ω so definiert sind, daß die drei Größen

$$\log k - \log 4 - \frac{\omega \pi i}{2} = \log k - \log 4\sqrt{q},$$

$$\log k' \quad \text{und} \quad \log \frac{2K}{\pi}$$

mit q unendlich klein werden.

Aus diesem Verhalten der Funktionen ergibt sich nun mit Hilfe der Transformation erster Ordnung der ϑ-Funktionen das von Riemann untersuchte Verhalten bei Annäherung von ω an einen reellen rationalen Wert, wobei q sich zugleich einer bestimmten Einheitswurzel q_0 nähert. Setzt man

$$\vartheta_1(z, \omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2 \frac{\omega}{2} + \left(s+\frac{1}{2}\right)\left(z-\frac{1}{2}\right)}$$
$$= 2\eta(\omega)\, 1^{\frac{\omega}{12}} \sin z\pi \Pi(1 - 1^{\omega\nu+\omega} z)(1 - 1^{\omega\nu-\omega} z),$$

wo die Summation auf alle ganzen Zahlen s auszudehnen ist, so wird, wenn man die nach z genommene Derivierte durch einen Akzent bezeichnet,

$$\vartheta_1'(0, \omega) = 2\pi\eta(\omega)^3.$$

Sind nun $\alpha, \beta, \gamma, \delta$ vier der Bedingung

$$\alpha\delta - \beta\gamma = 1 \tag{6}$$

genügende ganze Zahlen, so ist bekanntlich

$$\vartheta_1\left(z, \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c\sqrt{\alpha+\beta\omega}\, 1^{\frac{1}{2}\beta(\alpha+\beta\omega)z^2}\, \vartheta_1\Big((\alpha+\beta\omega)z, \omega\Big),$$

wo c eine von $\alpha, \beta, \gamma, \delta$ und der Wahl der Quadratwurzel abhängige achte Einheitswurzel bedeutet, deren Bestimmung von Hermite auf die Gaußschen Summen zurückgeführt ist (Liouvilles Journal, Serie II, T. III, 1858). Für $z = 0$ ergibt sich hieraus

$$\vartheta_1'\left(0, \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c(\alpha+\beta\omega)^{\frac{3}{2}}\, \vartheta_1'(0, \omega),$$

also

$$\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c^{\frac{1}{3}}(\alpha+\beta\omega)^{\frac{1}{2}}\, \eta(\omega), \tag{7}$$

und aus dieser Transformation von $\eta(\omega)$ ist diejenige von $\log\eta(\omega)$ abzuleiten.

Der Fall $\beta = 0$ erledigt sich unmittelbar durch die Definitionen (2) und (4) von $\eta(\omega)$, $log\,\eta(\omega)$ und gibt

$$log\,\eta(1+\omega) = log\,\eta(\omega) + \frac{\pi i}{12}, \tag{8}$$

oder allgemeiner, wenn n irgend eine ganze Zahl ist,

$$log\,\eta(n+\omega) = log\,\eta(\omega) + \frac{n\pi i}{12}. \tag{9}$$

Ist aber β von Null verschieden, so wird die Größe

$$\mu = -(\alpha+\beta\omega)^2$$

nirgends negativ, und man kann folglich $log\,\mu$ eindeutig so definieren, daß der imaginäre Bestandteil stets zwischen $\pm\pi i$ bleibt, und folglich konjugierten Werten von μ auch konjugierte Werte von $log\,\mu$ entsprechen; dann wird zufolge (7)

$$log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log\left\{-(\alpha+\beta\omega)^2\right\} + (\alpha,\beta,\gamma,\delta)\frac{\pi i}{12}, \tag{10}$$

wo $(\alpha, \beta, \gamma, \delta)$ eine durch $\alpha, \beta, \gamma, \delta$ vollständig bestimmte ganze Zahl bedeutet, welche dieselbe bleibt, wenn diese vier Zahlen mit (-1) multipliziert werden. Die vollständige Bestimmung dieser Zahl leistet offenbar noch sehr viel mehr, als die der obigen Einheitswurzel c, und bildet den eigentlichen Gegenstand der folgenden Untersuchung.

Zunächst läßt sich $(\alpha, \beta, \gamma, \delta)$ auf eine nur von α, β abhängige Zahl zurückführen. Genügen nämlich die Zahlen γ', δ' ebenfalls der Bedingung $\alpha\delta' - \beta\gamma' = 1$, so ist bekanntlich $\gamma' = \gamma + n\alpha$, $\delta' = \delta + n\beta$, wo n jede ganze Zahl bedeutet; mithin wird nach (9)

$$log\,\eta\left(\frac{\gamma'+\delta'\omega}{\alpha+\beta\omega}\right) = log\,\eta\left(n + \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) + \frac{n\pi i}{12},$$

und hieraus folgt nach (10), daß

$$(\alpha, \beta, \gamma', \delta') - \frac{\delta'}{\beta} = (\alpha, \beta, \gamma, \delta) - \frac{\delta}{\beta}$$

nur von den beiden Zahlen α, β abhängt; man kann daher

$$\beta(\alpha, \beta, \gamma, \delta) = \alpha + \delta - 2(\alpha, \beta), \tag{11}$$

also

$$log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log\left\{-(\alpha+\beta\omega)^2\right\} + \frac{\alpha+\delta-2(\alpha,\beta)}{12\beta}\,\pi i \tag{12}$$

setzen, wo $2(\alpha, \beta)$ und, wie sich später ergibt, auch (α, β) selbst eine ganze, lediglich von den beiden relativen Primzahlen α, β abhängende Zahl bedeutet; zugleich ergibt sich

$$(-\alpha, -\beta) = -(\alpha, \beta). \tag{13}$$

Ersetzt man ferner alle Glieder der Gleichung (12) durch die zugehörigen konjugierten Größen, so erhält man nach den obigen Bemerkungen

$$log\,\eta\left(-\frac{\gamma+\delta\omega'}{\alpha+\beta\omega'}\right) = log\,\eta(-\omega') + \frac{1}{4}log\left\{-(\alpha+\beta\omega')^2\right\} - \frac{\alpha+\delta-2(\alpha,\beta)}{12\beta}\pi i,$$

und da die linke Seite nach (12) auch in der Form

$$log\,\eta\left(\frac{-\gamma+\delta(-\omega')}{\alpha-\beta(-\omega')}\right) = log\,\eta(-\omega') + \frac{1}{4}log\left\{-(\alpha+\beta\omega')^2\right\} + \frac{\alpha+\delta-2(\alpha,-\beta)}{12(-\beta)}\pi i$$

dargestellt werden kann, so ergibt sich

$$(\alpha, -\beta) = (\alpha, \beta) \tag{14}$$

und zufolge (13) auch

$$(-\alpha, \beta) = -(\alpha, \beta). \tag{15}$$

Soll ferner der Satz (12) auch noch für den Fall $\beta = 0$, $\alpha = \delta = \pm 1$ gelten, so ist die Definition des Symbols (α, β) durch die Festsetzung

$$(\pm 1, 0) = \pm 1 \tag{16}$$

zu vervollständigen, welche auch mit (13), (14), (15) harmoniert.

Aus (15) folgt $(0, \pm 1) = 0$; setzt man daher $\alpha = 0$, $\beta = 1$, $\gamma = -1$, $\delta = 0$, so geht der Satz (12) über in den speziellen Fall der komplementären Transformation

$$log\,\eta\left(\frac{-1}{\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log(-\omega^2). \tag{17}$$

Ersetzt man nun in dem Satze (12) die Größe ω durch $1+\omega$ und durch $\frac{-1}{\omega}$, und drückt die Größen

$$log\,\eta\left(\frac{\gamma+\delta+\delta\omega}{\alpha+\beta+\beta\omega}\right) \quad \text{und} \quad log\,\eta\left(\frac{\delta-\gamma\omega}{\beta-\alpha\omega}\right)$$

wieder nach dem Satze (12) durch $log\,\eta(\omega)$ aus, so erhält man mit Rücksicht auf (8) und (17) leicht die beiden folgenden, für jedes Paar von relativen Primzahlen α, β geltenden Sätze

$$(\alpha+\beta, \beta) = (\alpha, \beta), \tag{18}$$

$$2\alpha(\alpha, \beta) + 2\beta(\beta, \alpha) = 1 + \alpha^2 + \beta^2 - 3|\alpha\beta|, \tag{19}$$

wo $|\alpha\beta|$ den absoluten Wert von $\alpha\beta$ bedeutet. Mit Zuziehung des letzteren Satzes, welcher in naher Beziehung zu dem Reziprozitätssatz in der Theorie der quadratischen Reste steht, kann man der Gleichung (11) auch die Form

(20) $$(\alpha, \beta, \gamma, \delta) = 2\gamma(\alpha, \beta) + 2\delta(\beta, \alpha) - (\alpha\gamma + \beta\delta) \pm 3\alpha\delta$$

geben, wo das Vorzeichen $\pm$ so zu wählen ist, daß $\pm\alpha\beta$ der absolute Wert von $\alpha\beta$ wird; hierdurch erscheint die zuerst in (10) auftretende Zahl $(\alpha, \beta, \gamma, \delta)$ wieder in Form einer ganzen Zahl.

Es leuchtet nun ein, daß die beiden Sätze (18) und (19) nicht nur die früheren Eigenschaften (13) bis (16) in sich schließen, sondern auch ausreichen, um in jedem Falle den Wert des Symbols (α, β) durch eine Kettenbruch-Entwicklung vollständig, und zwar als ganze Zahl zu bestimmen. Dies geht schon aus dem Satze

(21) $$(\alpha, \alpha + \beta) = (\alpha, \beta) - (\beta, \alpha) + \beta - \alpha, \quad \text{wenn} \quad \alpha\beta \geqq 0,$$

hervor, welcher leicht aus (18) und (19) abgeleitet wird; und umgekehrt leuchtet ein, daß dieser Satz (21) in Verbindung mit (18), d. h. mit dem Satze

(22) $$(\alpha', \beta) = (\alpha, \beta), \quad \text{wenn} \quad \alpha' \equiv \alpha \,(\text{mod. } \beta),$$

ebenfalls die vollständige Bestimmung des Symbols (α, β) enthält und eine sehr bequeme Berechnung einer Tabelle liefert. Es ist endlich sehr zweckmäßig, dem Symbol (α, β) auch dann eine bestimmte Bedeutung beizulegen, wenn die ganzen Zahlen α, β nicht relative Primzahlen sind, sondern einen beliebigen (positiven) größten gemeinsamen Teiler p haben; in diesem Falle setzen wir

(23) $$(\alpha, \beta) = p\left(\frac{\alpha}{p}, \frac{\beta}{p}\right),$$

weil dann offenbar die beiden Sätze (21), (22) ungeändert bestehen bleiben, während freilich das erste Glied 1 auf der rechten Seite des Satzes (19) durch p^2 zu ersetzen ist; aber in den beiden Sätzen (21), (22) ist jetzt auch ohne Zuziehung von (23) die vollständige Bestimmung von (α, β) enthalten, und sie gelten sogar für den Fall $\alpha = \beta = 0$, wenn

(24) $$(0, 0) = 0$$

gesetzt wird. Durch diese Erweiterung des Symbols (α, β) gelingt es oft, solche Sätze, die sonst in verschiedene Fälle zerfallen würden, in einem einzigen Ausspruch zu vereinigen (vgl. die in (28), (34) enthaltenen Sätze).

Obgleich nun das Symbol (α, β) durch die Eigenschaften (21), (22) für jedes Paar von ganzen rationalen Zahlen α, β vollständig bestimmt ist, so würde es doch schwer sein, aus ihnen einen allgemeinen Ausdruck für dasselbe abzuleiten. Mit Hilfe der von Riemann in dem zweiten Fragment angewandten Methode gelingt es aber, einen solchen Ausdruck in Form einer endlichen Summe aufzustellen. Diese Methode besteht in der Untersuchung des Verhaltens der Modulfunktionen, wenn $\omega = x + yi$ sich einem rationalen, in den kleinsten Zahlen ausgedrückten Bruche $\frac{-\alpha}{\beta}$ annähert. Geschieht diese Annäherung in der Weise, daß $\alpha + \beta x$ unendlich klein von höherer Ordnung wird als $\sqrt{y}$, so wird die Ordinate der in dem Satze (12) auftretenden Größe

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = \frac{\delta}{\beta} - \frac{1}{\beta(\alpha + \beta\omega)}$$

positiv unendlich groß, mithin nach (4)

$$log\,\eta(\omega_1) - \frac{\omega_1 \pi i}{12} = 0,$$

also

$$log\,\eta(\omega) + \frac{\pi i}{12\beta(\alpha + \beta\omega)} + \frac{1}{4} log\left\{-(\alpha + \beta\omega)^2\right\} = \frac{2(\alpha, \beta) - \alpha}{12\beta}\pi i;$$

ersetzt man, um sich der Bezeichnung von Riemann zu nähern, α, β durch $-m$, n, so kann man diesen Satz so aussprechen: Nähert sich die Variable $\omega = x + yi$ dem irreduzibelen Bruche $m:n$ so an, daß $nx - m$ von höherer Ordnung unendlich klein wird als $\sqrt{y}$, so wird zuletzt

$$(25) \qquad log\,\eta(\omega) + \frac{\pi i}{12n(n\omega - m)} + \frac{1}{4} log\left\{-(n\omega - m)^2\right\} = \frac{m - 2(m, n)}{12n}\pi i.$$

Unterwirft man aber die Annäherung der schärferen Bedingung, daß $nx - m$ von höherer Ordnung unendlich klein wird als y^2, so verschwinden gleichzeitig die imaginären Bestandteile des zweiten und dritten Gliedes links, und folglich ergibt sich durch Subtraktion der konjugierten Größen der Annäherungssatz

$$(26) \qquad log\,\eta(\omega) - log\,\eta(-\omega') = \frac{m - 2(m, n)}{6n}\pi i,$$

welcher zufolge der obigen Erweiterung des Symbols (m, n) auch dann gilt, wenn die ganzen Zahlen m, n irgendwelchen gemeinsamen Teiler haben.

Bevor wir denselben benutzen, um unsere Aufgabe zu lösen, bemerken wir noch folgendes. Sind a, d positive ganze Zahlen und c eine beliebige ganze Zahl, und genügt die Annäherung von ω an ihren rationalen Grenzwert der letzten, schärferen Bedingung, so gilt dasselbe offenbar auch für die Annäherung der Größe

$$\frac{c+d\omega}{a} \quad \text{an den Wert} \quad \frac{cn+dm}{an},$$

und folglich wird gleichzeitig mit (26) auch die Annäherung

$$log\,\eta\Big(\frac{c+d\omega}{a}\Big) - log\,\eta\Big(-\frac{c+d\omega'}{a}\Big) = \frac{cn+dm-2(cn+dm,\,an)}{6an}\pi i$$

eintreten. Nun besteht, wenn p eine Primzahl ist, der aus der Transformation $p$ter Ordnung oder aus (2) leicht abzuleitende Satz

$$(27) \qquad log\,\eta(p\omega) + \sum log\,\eta\Big(\frac{s+\omega}{p}\Big) = \frac{(p-1)\pi i}{24} + (p+1)\,log\,\eta(\omega),$$

wo s in der Summe die p Zahlen 0, 1, 2, $\cdots$, $(p-1)$ zu durchlaufen hat; zieht man hiervon die durch den Übergang zu den konjugierten Größen entstehende Gleichung ab, so ergibt sich durch die Grenzannäherung der Satz

$$(28) \qquad p(pm, n) + \sum (m + ns, np) = p(p+1)(m, n),$$

wo s ein beliebiges vollständiges Restsystem (mod. p) durchlaufen muß. Aus dem Satze (27) lassen sich auf verschiedene Weise allgemeinere Sätze ableiten, die für beliebige zusammengesetzte Zahlen p gelten, und aus jedem dieser Sätze entspringt wieder ein ähnlicher Satz über das Symbol (m, n); doch dürfen wir auf diese, an sich sehr interessanten Eigenschaften der Funktion $log\,\eta(\omega)$ und des Symbols (m, n) hier nicht eingehen.

Indem wir uns nun unserer Aufgabe zuwenden, benutzen wir die aus (2) und (4) folgende Darstellung

$$(29) \qquad log\,\eta(\omega) = \frac{\omega\pi i}{12} + \sum log\,(1 - 1^{\omega\nu}),$$

wo ν alle natürlichen Zahlen durchläuft, und die Logarithmen rechts zugleich mit 1^{ω} verschwinden; es wird daher

$$log\,(1 - 1^{\omega\nu}) = -\sum \frac{1^{\omega\nu\mu}}{\mu},$$

wo auch μ alle natürlichen Zahlen durchläuft, und wenn man die Summation nach ν ausführt, so erhält man die Umformung von Jacobi (Fund. nova § 39)

$$\log\eta(\omega) = \frac{\omega\pi i}{12} - \sum \frac{1}{\mu}\cdot\frac{1^{\omega\mu}}{1-1^{\omega\mu}}, \tag{30}$$

mithin

$$\log\eta(\omega) - \log\eta(-\omega') = \frac{(\omega+\omega')\pi i}{12} - \sum\frac{a_\mu}{\mu},$$

wo zur Abkürzung

$$a_\mu = \frac{1}{1-1^{\omega\mu}} - \frac{1}{1-1^{-\omega'\mu}}$$

gesetzt ist.

Jetzt lassen wir die positive Ordinate y der Größe $\omega = x + yi$ unendlich klein werden, während die Abszisse x von vornherein den konstanten rationalen Wert $m:n$ besitzen soll, wodurch die obige, schärfere Bedingung offenbar erfüllt ist. Die ganzen Zahlen m, n dürfen im folgenden einen beliebigen gemeinsamen Teiler haben, doch nehmen wir den Nenner n als positiv an. Setzen wir zur Abkürzung

$$1^x = 1^{\frac{m}{n}} = e^{\frac{2m\pi i}{n}} = \theta; \quad 1^{yi} = e^{-2\pi y} = r,$$

so genügt die Konstante θ der Bedingung $\theta^n = 1$, und r bedeutet einen variablen positiven echten Bruch, der wachsend sich dem Werte 1 annähert; zugleich ist

$$a_\mu = \frac{1}{1-\theta^\mu r^\mu} - \frac{1}{1-\theta^{-\mu}r^\mu},$$

und es handelt sich um die Bestimmung des Grenzwertes von

$$\log\eta(\omega) - \log\eta(-\omega') = \frac{m\pi i}{6n} - \sum\frac{a_\mu}{\mu}.$$

Durch Vereinigung von je zwei Zählern a_μ, welche den Zahlen $\mu = sn + \nu$ und $\mu = (s+1)n - \nu$ entsprechen, wo $0 < \nu < \frac{1}{2}n$, ergibt sich nun leicht, daß der absolute Betrag der Summe

$$A_\mu = a_1 + a_2 + \cdots + a_\mu$$

für alle Werte von r einschließlich $r = 1$ unterhalb einer von r und μ unabhängigen, endlichen Konstanten bleibt, und hieraus folgt nach einem allgemeinen Satze*), daß die Reihe

$$\sum\frac{a_\mu}{\mu} = \sum A_\mu\left(\frac{1}{\mu} - \frac{1}{\mu+1}\right),$$

*) Dirichlet, Vorlesungen über Zahlentheorie, 2. Aufl., § 143.

wenn ihre Glieder nach wachsenden μ geordnet werden, auch noch für $r = 1$ konvergiert und an dieser Stelle stetig ist; mit Rücksicht auf den Satz (26) ergibt sich daher

$$\frac{(m, n)\pi i}{3n} = \sum \frac{b_\mu}{\mu},$$

wo

$$b_\mu = \lim a_\mu = 0 \quad \text{oder} \quad = \frac{1}{1-\theta^\mu} - \frac{1}{1-\theta^{-\mu}},$$

je nachdem $\theta^\mu = 1$ ist oder nicht; durch Anwendung der Transformation

$$\frac{1}{1-\theta^\mu} = -\frac{1}{n} \sum \sigma \theta^{\mu\sigma},$$

wo σ die Werte $1, 2, \cdots, (n-1)$ durchläuft, erhält man aber die für alle μ geltende Darstellung

$$b_\mu = \frac{1}{n} \sum \sigma (\theta^{-\mu\sigma} - \theta^{\mu\sigma}),$$

aus welcher sich die Summe unserer unendlichen Reihe auch ohne Benutzung bestimmter Integrale sehr leicht ergibt.

Ist z irgend ein reeller Wert, so wollen wir den von z um eine ganze Zahl abstehenden, zwischen $\pm \frac{1}{2}$ liegenden Wert der Deutlichkeit halber nicht mit (z), sondern mit $((z))$ bezeichnen; für solche Werte von z aber, welche in der Mitte zwischen zwei ganzen Zahlen liegen, soll nach Riemann (S. 242 und 457)[*)] die hier unstetige periodische Funktion $((z)) = 0$, also gleich dem arithmetischen Mittel aus den beiden unendlich nahe benachbarten Werten $((z+0)) = -\frac{1}{2}$ und $((z-0)) = +\frac{1}{2}$ gesetzt werden. Nach einem sehr bekannten Satze aus der Theorie der trigonometrischen Reihen, der sich auch unmittelbar aus der Logarithmen-Reihe ergibt, gilt dann stets die Darstellung

$$2\pi i((z)) = \sum \frac{(-1)^\mu (1^{-z\mu} - 1^{z\mu})}{\mu},$$

wo μ die natürlichen Zahlen wachsend durchläuft, also auch

$$2\pi i\left(\left(z - \frac{1}{2}\right)\right) = \sum \frac{1^{-z\mu} - 1^{z\mu}}{\mu}. \tag{31}$$

[*) Die Seitenangaben beziehen sich auf die 2. Aufl. von B. Riemanns ges. mathem. Werken usw.]

Hieraus folgt

$$\sum \frac{\theta^{-\mu\sigma} - \theta^{\mu\sigma}}{\mu} = 2\pi i\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right),$$

mithin

$$\frac{(m, n)}{6n} = \sum \frac{\sigma}{n}\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right);$$

da aber, wie sich durch Verwandlung von σ in $n - \sigma$ ergibt,

$$\frac{1}{2}\sum\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right) = 0$$

ist, so erhält man hieraus leicht durch Subtraktion den folgenden Ausdruck

$$(32) \qquad (m, n) = 6n \sum \left(\left(\frac{s}{n} - \frac{1}{2}\right)\right)\left(\left(\frac{ms}{n} - \frac{1}{2}\right)\right),$$

wo n positiv angenommen ist, und s ein beliebiges vollständiges Restsystem (mod. n) durchläuft. Dieser Ausdruck für das Symbol (m, n) in Form einer endlichen Summe gestattet noch manche Umformungen und Vereinfachungen, auf welche wir unten noch näher eingehen wollen. Daß derselbe auch dann gilt, wenn die Zahlen m, n einen beliebigen (positiven) gemeinschaftlichen Teiler p haben, läßt sich mit Rücksicht auf (23) nachträglich mit Hilfe des auch sonst wichtigen Satzes

$$(33) \qquad \sum\left(\left(\frac{x + p'}{p} - \frac{1}{2}\right)\right) = \left(\left(x - \frac{1}{2}\right)\right)$$

leicht bestätigen, in welchem x eine beliebige reelle Zahl bedeutet und p' ein vollständiges Restsystem (mod. p) durchläuft.

Machen wir jetzt die Voraussetzung, daß m, n relative Primzahlen sind, und setzen wir zur Abkürzung

$$B = \frac{\pi i}{24n(n\omega - m)}, \quad C = \frac{1}{4} log\left\{-(n\omega - m)^2\right\},$$

$$\mu = \frac{1 - (-1)^m}{2}, \qquad \nu = \frac{1 - (-1)^n}{2},$$

so ist $(1 - \mu)(1 - \nu) = 0$, $m \equiv \mu$, $n \equiv \nu$ (mod. 2), und aus dem Annäherungs-Satze (25)

$$log\,\eta(\omega) = \frac{m - 2(m, n)}{12n}\pi i - 2B - C$$

folgt gleichzeitig

$$\log\eta(2\omega) = \frac{m-(2m,n)}{6n}\pi i-(4-3\nu)B-C+\frac{\nu}{2}\log 2,$$

$$\log\eta\left(\frac{\omega}{2}\right) = \frac{m-2(m,2n)}{24n}\pi i-(4-3\mu)B-C+\frac{1-\mu}{2}\log 2,$$

$$\log\eta\left(\frac{1+\omega}{2}\right) = \frac{m+n-2(m+n,2n)}{24n}\pi i+(2-3\mu-3\nu)B-C+\frac{\mu+\nu-1}{2}\log 2;$$

die hier auftretenden Symbole sind zufolge (28) durch die stets geltende Relation

(34) $$2(2m,n)+(m,2n)+(m+n,2n) = 6(m,n)$$

miteinander verbunden. Gleichzeitig ergeben sich hieraus zufolge (5) die Annäherungen

(35)
$$\begin{cases} \log k = \frac{3m+2(m+n,2n)-4(2m,n)}{6n}\pi i+(\mu+2\nu-2)(12B-2\log 2), \\ \log k' = \frac{(m+n,2n)-(m,2n)}{3n}\pi i+(2\mu+\nu-2)(12B-2\log 2), \\ \log\frac{2K}{\pi} = \frac{(m,n)-(m+n,2n)}{3n}\pi i+(1-\mu-\nu)(12B-2\log 2)-2C. \end{cases}$$

Die Vergleichung dieser Sätze mit den acht Formeln des zweiten Fragments ergibt, daß Riemann auf die Bestimmung der unendlich großen reellen Bestandteile, welche in den Gliedern mit B, C enthalten sind, weniger Wert gelegt hat; sie sind zum Teil ungenau dargestellt, zum Teil ganz weggelassen. Auch in den imaginären Bestandteilen fanden sich (bei der dritten, vierten und fünften Formel) einige kleine Versehen, die sich aber ohne Zwang schon in der ersten Auflage berichtigen ließen, während die reellen Teile auch jetzt ungeändert abgedruckt werden. Daß die Riemannschen Formeln in den imaginären Bestandteilen mit den vorstehenden Sätzen (35) übereinstimmen, ist nicht überall auf den ersten Blick zu erkennen, und es würde zu weit führen, diese Übereinstimmung hier vollständig nachzuweisen; doch wollen wir, weil der Gegenstand wichtig genug ist, zur Erleichterung noch folgende Bemerkungen hinzufügen.

Unter dem Nenner einer rationalen Zahl x verstehen wir immer die kleinste positive ganze Zahl n, für welche das Produkt nx ebenfalls eine ganze Zahl m wird, und diese nennen wir den Zähler von x. Es gibt dann immer unendlich viele Zahlen x', welche denselben Nenner n haben, und deren Zähler m' der Kongruenz $mm' \equiv 1 \pmod{n}$

genügen, und jede solche Zahl x' soll ein Gefährte (socius) von x heißen (vgl. Art. 77 der Disqu. Arithm.). Nennt man zwei Zahlen x, y schlechthin kongruent, wenn ihre Differenz eine ganze Zahl ist, und bezeichnet dies durch $x \equiv y$, so entspricht jeder Klasse von kongruenten Zahlen x eine und nur eine Klasse von Zahlen x', und wenn p eine ganze Zahl, und zwar relative Primzahl zu n bedeutet, so ist $p(px')' \equiv x$. Setzen wir nun zur Abkürzung

$$(36) \qquad D(x) = \frac{(m,n)}{n} = 6\sum\left(\left(\frac{s}{n}-\frac{1}{2}\right)\right)\left(\left(\frac{ms}{n}-\frac{1}{2}\right)\right),$$

so hat diese Funktion, wie sich aus dem vorstehenden Ausdrucke, oder auch aus (18), (15), (12), (34) leicht ergibt, die Eigenschaften

$$(37) \qquad \begin{cases} D(x) = D(x+1) = -D(-x) = D(x'), \\ D(2x) + D\left(\frac{x}{2}\right) + D\left(\frac{x+1}{2}\right) = 3D(x). \end{cases}$$

Ersetzt man die in den Riemannschen Formeln bisweilen benutzte Funktion $E(x)$, welche die größte in x enthaltene ganze Zahl bedeutet, durch den Ausdruck

$$(38) \qquad E(x) = x - \frac{1}{2} - \left(\left(x - \frac{1}{2}\right)\right),$$

in welchem nur, wenn x selbst eine ganze Zahl ist, statt $E(x)$ wieder das arithmetische Mittel $x - \frac{1}{2}$ aus $E(x+0)$ und $E(x-0)$ zu nehmen ist, so treten in den meisten dieser Formeln zuletzt nur noch Funktionen von der Form

$$(39) \qquad R(x) = \sum((\nu x)), \quad S(x) = \sum\left(\left(\nu x - \frac{1}{2}\right)\right)$$

auf, wo die Summationen sich auf alle diejenigen, nicht negativen ganzen Zahlen ν beziehen, welche kleiner als der halbe Nenner von x sind; diese Funktionen haben die Eigenschaften

$$(40) \qquad \begin{cases} R(x) = R(x+1) = -R(-x) \\ S(x) = S(x+1) = -S(-x) \\ R(x) - S(x) = R(x') - S(x') = \frac{1}{2}h, \end{cases}$$

wo h den Überschuß der Anzahl der positiven Glieder $((\nu x))$ über die der negativen bedeutet, und stehen in folgenden Beziehungen zu der Funktion $D(x)$. Allgemein ist nach (36)

$$(41) \qquad 6S(x') = D(2x) - 2D(x).$$

Hat die Zahl x einen geraden Nenner n, so ist

$$(42)\quad \begin{cases} R(x) = -S(x) = \frac{1}{4}h = \frac{1}{3}D(x) - \frac{1}{6}D(2x), \\ R\left(\frac{x}{2}\right) + R\left(\frac{x+1}{2}\right) = 2R(x). \end{cases}$$

Hat aber die Zahl x einen ungeraden Nenner n, so zerfallen die Zahlen y, welche der Bedingung $2y \equiv x$ genügen, also $\equiv \frac{1}{2}x$ oder $\equiv \frac{1}{2}(x+1)$ sind, in zwei Klassen von Zahlen, von denen diejenigen, welche denselben Nenner n haben, mit x_1, die übrigen mit x_2 bezeichnet werden sollen; die letzteren haben den Nenner $2n$. Dann ist

$$(43)\qquad R(x_2) = R(x) - S(x) = 2R(x) - S(2x)$$

und

$$(44)\quad \begin{cases} D(x) &= 6R(x_2) - 4R(x) - 4R(x'), \\ D(2x) &= 6R(x_2) - 8R(x) - 2R(x'), \\ D(x_1) &= 6R(x_2) - 2R(x) - 8R(x'), \\ D(x_2) &= 6R(x_2) - 2R(x) - 2R(x'), \end{cases}$$

wodurch wieder die obige Bedingung

$$(45)\qquad D(2x) + D(x_1) + D(x_2) = 3D(x)$$

erfüllt wird. Die Übereinstimmung der drei ersten Darstellungen in (44) ergibt sich aus den früheren Eigenschaften von $R(x)$ mit Rücksicht auf die Beziehungen

$$x_1 \equiv x_2 + \frac{1}{2} \equiv (2x')', \quad \left(x + \frac{1}{2}\right)' \equiv (4x)' + \frac{1}{2}, \quad (x_2)' \equiv (x')_2;$$

und umgekehrt ist

$$(46)\quad \begin{cases} 6R(x) &= 3D(x) - 2D(2x) - D(x_1) = D(x_2) - D(2x) \\ 6R(x') &= 3D(x) - D(2x) - 2D(x_1) = D(x_2) - D(x_1) \\ 6R(x_2) &= 5D(x) - 2D(2x) - 2D(x_1) = 2D(x_2) - D(x). \end{cases}$$

Die Herleitung dieser und zahlreicher anderer Relationen, welche alle in naher Beziehung zu der Theorie der quadratischen Reste stehen, müssen wir uns aber für eine andere Gelegenheit versparen.

Erläuterungen zur vorstehenden Abhandlung.

Die Bedeutung der Abhandlung geht weit hinaus über ihre erste Absicht, nur eine Erläuterung zu den beiden Riemannschen „Fragmenten über die Grenzfälle der elliptischen Modulfunktionen“ sein zu wollen. Die Methoden der Abhandlung führen nicht nur zur Bestimmung derjenigen bei der linearen Transformation der ϑ-Funktionen auftretenden Einheitswurzeln, die bereits von Jacobi und Hermite berechnet wurden (vgl. den Anfang der Abhandlung), sondern auch zur Bestimmung der 24sten Einheitswurzel, die bei der linearen Transformation der 24sten Wurzel der Diskriminante

$$\sqrt[24]{\Delta(\omega_1, \omega_2)} = \sqrt{\frac{2\pi}{\omega_2}}\,\eta(\omega)$$

auftritt. Über den letzteren Gegenstand vgl. man die Dissertation von Th. Molien: „Über die lineare Transformation der elliptischen Funktionen“ (Dorpat, 1885).

Das Problem Dedekinds umfaßt sofort alle Wurzeln aus η, indem er das Verhalten der in der positiven ω-Halbebene eindeutigen Funktion $\log \eta(\omega)$ gegenüber der Modulgruppe festzustellen anstrebt. Das Problem wird zurückgeführt auf die Bestimmung der durch das Symbol (m, n) bezeichneten ganzen Zahl. Es wird zunächst die Berechnung von (m, n) durch ein Kettenbruchverfahren gelehrt und sodann eine allgemein gültige Darstellung von (m, n) in einer endlichen Summe mittels des Restsymbols $((x))$ entwickelt.

Dedekind betont den Zusammenhang des Symbols (m, n) mit der Theorie der quadratischen Reste und hat demselben mit Recht überhaupt eine große zahlentheoretische Bedeutung zuerkannt. Aber auch die Darstellung von (m, n) durch das Restsymbol $((x))$ gibt noch keineswegs einen tieferen Einblick in die Abhängigkeit der ganzen Zahl (m, n) von m und n. Man weiß lediglich, daß die Zahlen (m, n) mod 24 mit gewissen rationalen Ausdrücken in m und n kongruent sind. Es hängt dies, um beim Legendreschen Integralmodul k^2 zu bleiben, mit dem Umstand zusammen, daß von allen Wurzeln aus k^2 nur k^2, k, $\sqrt{k}$ und $\sqrt[4]{k}$ sogenannte „Kongruenzmoduln“ sind, d. h. daß sich nur die zu ihnen gehörenden Teiler der Modulgruppe durch Kongruenzen erklären lassen. Es sind Versuche gemacht, zu arithmetischen Aussagen über die zu höheren Wurzeln aus k^2 gehörenden Teiler der Modulgruppe zu gelangen. Diese Versuche schlossen mit dem negativen Ergebnis, daß diese Teiler eben „Nicht-Kongruenzgruppen“ seien, worüber die Arbeiten von G. Pick, Mathem. Ann., Bd. 28, S. 119 (1886) und R. Fricke, ebenda, Bd. 28, S. 99 (1886) zu vergleichen sind. Von einer tieferen Erforschung des Dedekindschen Symbols (m, n) darf man neue Aufschlüsse in dieser Richtung erwarten.

Fricke.

XIV.

Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen.

[Journal für reine und angewandte Mathematik, Bd. 83, S. 265—292 (1877)].

Sie haben mich aufgefordert, eine etwas ausführlichere Darstellung der Untersuchungen auszuarbeiten, von welchen ich, durch das Erscheinen der Abhandlung von Fuchs*) veranlaßt, mir neulich erlaubt habe Ihnen eine kurze Übersicht mitzuteilen; indem ich Ihrer Einladung hiermit Folge leiste, beschränke ich mich im wesentlichen auf den Teil dieser Untersuchungen, welcher mit der eben genannten Abhandlung zusammenhängt, und ich bitte Sie auch, die Übergehung einiger Nebenpunkte entschuldigen zu wollen, da es mir im Augenblick an Zeit fehlt, alle Einzelheiten auszuführen. Die in Rede stehenden Untersuchungen habe ich schon vor einer Reihe von Jahren angestellt, als ich erkannte, daß die Bestimmung der Anzahl der Idealklassen in kubischen Körpern (d. h. in Gebieten von Zahlen, welche aus Wurzeln von Gleichungen dritten Grades gebildet sind) innig zusammenhängt mit der Theorie der singulären Moduln der elliptischen Funktionen, für welche die komplexe Multiplikation stattfindet. Bei meinen Versuchen, tiefer in diese mir unentbehrliche Theorie einzudringen und mir einen einfachen Weg zu den ausgezeichnet schönen Resultaten von Kronecker zu bahnen, die leider noch immer so schwer zugänglich sind, erkannte ich sogleich die fundamentale Wichtigkeit des Punktes, auf welchen auch Hermite neulich in einer Anmerkung zu der Abhandlung von Fuchs (S. 29) aufmerksam gemacht hat, und welcher in der Tat zur Grundlage für meine Theorie geworden ist. Es handelt sich um folgendes. Bedeutet

$$\omega = \frac{K' i}{K}$$

[*) Journ. f. reine u. angew. Mathem., Bd. 83, S. 13—37.]

das Periodenverhältnis der elliptischen Funktionen (= Hi nach der Bezeichnung von Fuchs), so ist das Quadrat $k = \varkappa^2$ des Integralmoduls $\varkappa$ eine einwertige Funktion von ω, welche Hermite mit $\varphi(\omega)^8$ bezeichnet, und aus der Transformation erster Ordnung folgt leicht, daß k unverändert bleibt, wenn ω durch

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

ersetzt wird, wo α, β, γ, δ vier ganze rationale Zahlen bedeuten, welche der Bedingung

$$\alpha\delta - \beta\gamma = 1$$

genügen, und von denen β, γ gerade sind. Der zu beweisende Satz besteht nun darin, daß außer diesen Zahlen ω_1 keine andere existiert, welche denselben Wert $k = \varphi(\omega)^8 = \varphi(\omega_1)^8$ hervorbringt. Bevor ich zur Darstellung meiner Theorie übergehe, will ich zunächst zeigen, daß dieser Satz sich auch aus der gewöhnlichen Theorie der elliptischen Funktionen ohne Schwierigkeit ableiten läßt.

Bedeutet ω eine komplexe Größe mit positiv-imaginärem Bestandteil, ferner z eine willkürliche Variable, und bedient man sich der folgenden Bezeichnungen

$$1^z = e^{2\pi i z},$$

$$\vartheta(z, \omega) = \sum 1^{s^2\frac{\omega}{2} + s\left(z - \frac{1}{2}\right)},$$

$$\vartheta_1(z, \omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2\frac{\omega}{2} + \left(s+\frac{1}{2}\right)\left(z-\frac{1}{2}\right)},$$

$$\vartheta_2(z, \omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2\frac{\omega}{2} + \left(s+\frac{1}{2}\right)z},$$

$$\vartheta_3(z, \omega) = \sum 1^{s^2\frac{\omega}{2} + sz},$$

wo s alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchläuft, ferner

$$\sqrt{\varkappa} = \frac{\vartheta_2(0, \omega)}{\vartheta_3(0, \omega)} = \varphi(\omega)^2; \quad \sqrt{\varkappa'} = \frac{\vartheta(0, \omega)}{\vartheta_3(0, \omega)} = \psi(\omega)^2,$$

so ist

$$\varkappa^2 + \varkappa'^2 = 1,$$

und man kann

$$\sqrt{x} = \frac{1}{\sqrt{\varkappa}} \frac{\vartheta_1(z, \omega)}{\vartheta(z, \omega)} = sin\, am(2Kz, \varkappa),$$

$$\sqrt{1 - x} = \frac{\sqrt{\varkappa'}}{\sqrt{\varkappa}} \frac{\vartheta_2(z, \omega)}{\vartheta(z, \omega)} = cos\, am(2Kz, \varkappa),$$

$$\sqrt{1 - \varkappa^2 x} = \sqrt{\varkappa'} \frac{\vartheta_3(z, \omega)}{\vartheta(z, \omega)} = \Delta am(2Kz, \varkappa),$$

$$\frac{d\sqrt{x}}{dz} = 2K\sqrt{1 - x}\sqrt{1 - \varkappa^2 x}$$

setzen, wo

$$2K = \frac{\vartheta_3(0,\omega)\vartheta_1'(0,\omega)}{\vartheta(0,\omega)\vartheta_2(0,\omega)} = \pi\vartheta_3(0,\omega)^2$$

ist. Wenn nun die Größe ω_1 ebenfalls einen positiv-imaginären Bestandteil hat und denselben Wert

$$\frac{\vartheta_2(0,\omega_1)^4}{\vartheta_3(0,\omega_1)^4} = x_1^2 = x^2 = k$$

hervorbringt, wie ω, so setze man

$$2K_1 = \pi\vartheta_3(0,\omega_1)^2$$

und führe eine neue Variable z_1 durch die Gleichung

$$K_1 z_1 = Kz$$

ein; wenn ferner mit $\sqrt{x_1}$, $\sqrt{1-x_1}$, $\sqrt{1-kx_1}$ die Größen bezeichnet werden, welche ebenso von z_1, ω_1 abhängen, wie $\sqrt{x}$, $\sqrt{1-x}$, $\sqrt{1-kx}$ von z, ω, so ergibt sich

$$\frac{d\sqrt{x}}{\sqrt{1-x}\sqrt{1-kx}} = \frac{d\sqrt{x_1}}{\sqrt{1-x_1}\sqrt{1-kx_1}},$$

und hieraus durch Integration

$$\sqrt{x}\sqrt{1-x_1}\sqrt{1-kx_1} - \sqrt{x_1}\sqrt{1-x}\sqrt{1-kx} = C(1-kxx_1);$$

die Konstante C muß aber gleich Null sein, weil für $z=0$ auch $z_1=0$ ist, also $\sqrt{x}$ und $\sqrt{x_1}$ gleichzeitig verschwinden. Hieraus folgt, daß identisch $x = x_1$ ist (ja sogar $\sqrt{x} = \sqrt{x_1}$, $\sqrt{1-x} = \sqrt{1-x_1}$, $\sqrt{1-kx} = \sqrt{1-kx_1}$); mithin wird jede der vier Funktionen

$$\vartheta(z,\omega),\quad \vartheta_1(z,\omega),\quad \vartheta_2(z,\omega),\quad \vartheta_3(z,\omega)$$

stets und nur dann verschwinden, wenn die entsprechende der vier Funktionen

$$\vartheta(z_1,\omega_1),\quad \vartheta_1(z_1,\omega_1),\quad \vartheta_2(z_1,\omega_1),\quad \vartheta_3(z_1,\omega_1)$$

verschwindet. Die Funktion $\vartheta_1(z,\omega)$ verschwindet aber für alle Werte $z = r + s\omega$ und nur*) für diese, wo r, s willkürliche ganze Zahlen bedeuten; setzt man daher

$$z_1 = 1,\quad \text{so wird}\quad z = \frac{K_1}{K} = \alpha + \beta\omega,$$

$$z_1 = \omega_1,\quad \text{so wird}\quad z = \frac{K_1}{K}\omega_1 = \gamma + \delta\omega,$$

*) Dies folgt aus der Darstellung von $\vartheta_1(z,\omega)$ als unendliches Produkt, oder auch aus dem Satze $\int d\log\vartheta_1(z,\omega) = 2\pi i$, wo die Integration durch die Begrenzung eines elementaren Parallelogramms erstreckt ist.

wo α, β, γ, δ ganze rationale Zahlen bedeuten; mithin ist

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad (\alpha + \beta\omega) z_1 = z. \tag{1}$$

Setzt man umgekehrt

$$z = 1, \text{ so wird } z_1 = \alpha_1 + \beta_1\omega_1$$
$$z = \omega, \text{ so wird } z_1 = \gamma_1 + \delta_1\omega_1,$$

wo α_1, β_1, γ_1, δ_1 ebenfalls ganze Zahlen bedeuten; es wird daher

$$(\alpha + \beta\omega)\alpha_1 + (\gamma + \delta\omega)\beta_1 = 1,$$
$$(\alpha + \beta\omega)\gamma_1 + (\gamma + \delta\omega)\delta_1 = \omega,$$

woraus, weil ω nicht reell ist,

$$\alpha\alpha_1 + \gamma\beta_1 = 1, \quad \beta\alpha_1 + \delta\beta_1 = 0,$$
$$\alpha\gamma_1 + \gamma\delta_1 = 0, \quad \beta\gamma_1 + \delta\delta_1 = 1,$$

also

$$(\alpha\delta - \beta\gamma)(\alpha_1\delta_1 - \beta_1\gamma_1) = 1,$$

mithin

$$\alpha\delta - \beta\gamma = \alpha_1\delta_1 - \beta_1\gamma_1 = \pm 1$$

folgt*). Hierin darf aber zufolge (1) nur das obere Zeichen genommen werden, weil der Koeffizient von i in beiden Größen ω und ω_1 dasselbe (positive) Vorzeichen hat; also ist

$$\alpha\delta - \beta\gamma = +1. \tag{2}$$

Da ferner die Werte von z_1, für welche $\vartheta(z_1, \omega_1)$ verschwindet, mit den Werten $r + (s + \frac{1}{2})\omega_1$ zusammen fallen, so wird gleichzeitig

$$z = \frac{\omega}{2}, \quad z_1 = r + (s + \tfrac{1}{2})\omega_1;$$

mithin ist zufolge (1)

$$(\alpha + \beta\omega) r + (\gamma + \delta\omega)(s + \tfrac{1}{2}) = \frac{\omega}{2},$$
$$\alpha r + \gamma(s + \tfrac{1}{2}) = 0,$$

also

$$\gamma \equiv 0 \pmod 2. \tag{3}$$

Auf dieselbe Weise ergibt sich aus dem gleichzeitigen Verschwinden der Funktionen $\vartheta_2(z, \omega)$, $\vartheta_2(z_1, \omega_1)$ für $z = \frac{1}{2}$ auch

$$\beta \equiv 0 \pmod 2, \tag{4}$$

womit der in Rede stehende Satz vollständig bewiesen ist.

Dieser Beweis beruht offenbar darauf, daß die elliptischen Funktionen $sin\,am(u, \varkappa)$, $cos\,am(u, \varkappa)$, $\Delta am(u, \varkappa)$ einwertige Funktionen auch von $k = \varkappa^2$ sind. Der Satz selbst reizte mich aber bald, den

*) Dies ist nur ein spezieller Fall eines allgemeinen Satzes aus der Theorie der Zahlensysteme, welche ich *endliche Moduln* genannt habe.

Zusammenhang zwischen den Größen ω, k, K ganz unabhängig von der Theorie der elliptischen Funktionen zu erforschen, und in diesem Streben bestärkte mich eine Bemerkung von Hermite, welcher an einer Stelle seiner kurzen Übersicht über die Theorie der elliptischen Funktionen hervorhebt, daß noch kein anderer Weg zu diesen Modulfunktionen führe, als der, welchen die Gründer der Theorie der elliptischen Funktionen eingeschlagen haben. Ich erlaube mir nun, Ihnen meine damals entstandene Theorie in ihren Grundzügen zu entwickeln; die Anwendung auf die Theorie der singulären Moduln, derentwegen die ganze Untersuchung angestellt ist, darf ich Ihnen vielleicht ein anderes Mal vorlegen.

§ 1.

Äquivalente Zahlen.

Zwei Zahlen ω, ω_1 sollen im folgenden *äquivalent* heißen, wenn es vier ganze (rationale) Zahlen α, β, γ, δ gibt, welche den beiden Bedingungen

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha\delta - \beta\gamma = 1$$

genügen; offenbar ist die hierdurch ausgedrückte Beziehung zwischen ω, ω_1 eine gegenseitige, da zugleich die vier Zahlen δ, $-\beta$, $-\gamma$, α den Bedingungen

$$\omega = \frac{(-\gamma) + \alpha\omega_1}{\delta + (-\beta)\omega_1}, \quad \delta\alpha - (-\beta)(-\gamma) = 1$$

genügen. Ist nun ω_2 ebenfalls äquivalent mit ω, gibt es also vier ganze Zahlen α_1, β_1, γ_1, δ_1, welche den Bedingungen

$$\omega = \frac{\gamma_1 + \delta_1\omega_2}{\alpha_1 + \beta_1\omega_2}, \quad \alpha_1\delta_1 - \beta_1\gamma_1 = 1$$

genügen, so setze man in üblicher Weise

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\begin{pmatrix}\alpha_1, \beta_1\\ \gamma_1, \delta_1\end{pmatrix} = \begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix},$$

d. h.

$$\alpha' = \alpha\alpha_1 + \beta\gamma_1, \quad \beta' = \alpha\beta_1 + \beta\delta_1,$$
$$\gamma' = \gamma\alpha_1 + \delta\gamma_1, \quad \delta' = \gamma\beta_1 + \delta\delta_1;$$

da diese Zahlen α', β', γ', δ' den beiden Bedingungen

$$\omega_1 = \frac{\gamma' + \delta'\omega_2}{\alpha' + \beta'\omega_2}, \quad \alpha'\delta' - \beta'\gamma' = 1$$

genügen, so folgt, daß je zwei mit einer und derselben Zahl ω äquivalente Zahlen ω_1, ω_2 auch miteinander äquivalent sind. Aus diesem Grunde wird man das gesamte Zahlengebiet in Klassen einteilen können, indem man je zwei Zahlen in dieselbe oder in zwei verschiedene Klassen aufnimmt, je nachdem sie äquivalent sind oder nicht. Jede Zahl ω kann als Repräsentant derjenigen Klasse angesehen werden, welche aus allen mit ω äquivalenten Zahlen besteht.

Nennt man die reellen Zahlen x, y die Koordinaten, und zwar x die Abszisse, y die Ordinate der aus ihnen gebildeten komplexen Zahl $\omega = x + yi$, so ergibt sich leicht, daß die Ordinaten von je zwei äquivalenten Zahlen ω, ω_1 dasselbe Vorzeichen haben, oder beide verschwinden. Wir werden im folgenden das Gebiet S derjenigen ω betrachten, deren Ordinaten positiv sind, und außerdem nur noch die rationalen reellen Zahlen, welche letzteren offenbar eine einzige Klasse R bilden, weil sie sämtlich mit der Zahl 0 äquivalent sind; es wird sich zeigen, daß diese Klasse R, welche zugleich die Zahl ∞ enthält, als die vollständige Begrenzung des Gebietes S anzusehen ist.

§ 2.

Vollständiges Repräsentantensystem.

Es kommt nun darauf an, ein vollständiges System von Repräsentanten ω_0 aller Klassen aufzustellen, aus welchen das Gebiet S besteht, in der Weise, daß jede Zahl ω dieses Gebietes mit einem, und im allgemeinen auch nur mit einem dieser Repräsentanten ω_0 äquivalent ist. Dies geschieht durch den folgenden Satz, in welchem das Zeichen $N(x + yi)$ die Norm $(x^2 + y^2)$ der komplexen Zahl $x + yi$ bedeutet:

In jeder Klasse des Gebietes S einschließlich R gibt es einen, und im allgemeinen auch nur einen Repräsentanten ω_0, welcher den drei Bedingungen

(1) $$N(\omega_0 - 1) \geqq N(\omega_0),$$

(2) $$N(\omega_0 + 1) \geqq N(\omega_0),$$

(3) $$N(\omega_0) \geqq 1$$

genügt.

Der Beweis kann mit denselben Mitteln geführt werden, durch welche in der Theorie der binären quadratischen Formen von negativer Determinante bewiesen wird, daß jede solche Form einer, und

im allgemeinen auch nur einer reduzierten Form äquivalent ist. Ich will mich hier begnügen, den ersten Teil des Satzes durch die folgende Betrachtung zu erledigen. Ist ω eine bestimmte Zahl des Gebietes S, so gibt es, weil ω nicht reell ist, unter allen Paaren von relativen Primzahlen α, β mindestens eins, für welches $N(\alpha + \beta\omega)$ so klein wie möglich wird; nachdem α, β so gewählt sind, erhält man alle Lösungen der Gleichung $\alpha\delta - \beta\gamma = 1$ in ganzen Zahlen γ, δ aus einer einzigen Lösung γ', δ', indem man $\gamma = \gamma' - m\alpha$, $\delta = \delta' - m\beta$ setzt und m alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchlaufen läßt; wählt man m so, daß

$$N\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = N\left(\frac{\gamma' + \delta'\omega}{\alpha + \beta\omega} - m\right)$$

möglichst klein wird, so hat die mit ω äquivalente Zahl

$$\omega_0 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

die in (1), (2), (3) ausgedrückten Eigenschaften. Denn aus der Definition von α, β folgt, daß ω_0 der Bedingung (3) genügt, und ebenso aus der Definition von m, daß ω_0 den Bedingungen (1) und (2) genügt.

Geometrisch wird der Inbegriff aller dieser Zahlen ω_0 durch ein Stück der Halbebene S dargestellt, welches das Hauptfeld heißen und mit (ω_0) bezeichnet werden soll. Dasselbe ist begrenzt durch drei Linien, welche den Gleichheitszeichen in den Bedingungen (1), (2), (3) entsprechen; setzt man $\omega_0 = x_0 + y_0 i$, so nehmen die letzteren die folgende Gestalt an:

(1) $\quad x_0 \leqq \frac{1}{2}$,

(2) $\quad x_0 \geqq -\frac{1}{2}$,

(3) $\quad x_0^2 + y_0^2 \geqq 1$;

das Feld (ω_0) liegt daher zwischen den beiden Geraden, welche in den Abständen $\pm\frac{1}{2}$ parallel mit der Ordinatenachse laufen, und zugleich außerhalb des Halbkreises, welcher mit dem Radius Eins aus dem Nullpunkte beschrieben ist. Dieses Feld wird offenbar durch die Ordinatenachse in zwei symmetrische Hälften zerlegt. Die beiden Parallelen (2) und (1) schneiden sich im Punkte ∞, dem Repräsentanten der Klasse R der rationalen Zahlen, und sie schneiden den Kreis in den Punkten

$$\varrho = \frac{-1 + i\sqrt{3}}{2} \quad \text{und} \quad -\varrho^2 = 1 + \varrho = \frac{-1}{\varrho},$$

während die Symmetrieachse den Kreis im Punkte

$$i = \frac{-1}{i}$$

schneidet.

Wenn nun ω_0 der Grenzlinie (2) angehört, d. h. wenn $x_0 = -\frac{1}{2}$ ist, so leuchtet ein, daß die äquivalente Zahl $1 + \omega_0$ der Grenzlinie (1) angehört, und diese beiden Punkte ω_0, $1 + \omega_0$ liegen symmetrisch zu beiden Seiten der Ordinatenachse. Wenn ferner ω_0 der Kreislinie (3) angehört, so gilt dasselbe von der äquivalenten Zahl $\frac{-1}{\omega_0} = -x_0 + y_0 i$, und diese beiden Punkte ω_0, $\frac{-1}{\omega_0}$ liegen ebenfalls symmetrisch zu beiden Seiten der Ordinatenachse. Je zwei symmetrische Punkte der Begrenzung von (ω_0) sind daher Repräsentanten einer und derselben Klasse. Es ließe sich nun auch leicht zeigen, daß außer diesen Fällen niemals zwei verschiedene Punkte oder Zahlen des Feldes (ω_0) derselben Klasse angehören können, mögen sie im Innern oder auf der Begrenzung von (ω_0) liegen. Der Kürze halber unterdrücke ich diesen Beweis, welcher, wie schon oben bemerkt, genau ebenso lautet, wie der Beweis des Satzes, daß zwei verschiedene reduzierte binäre quadratische Formen von negativer Determinante nur in gewissen Ausnahmefällen äquivalent sein können (vgl. Zahlentheorie von Dirichlet, zweite Auflage, § 65); es wird genügen zu bemerken, daß, wenn x, y willkürliche Variable bedeuten, die binäre quadratische Form

$$N(x + y\omega_0) = (1, x_0, x_0^2 + y_0^2),$$

deren Determinante $= -y_0^2$, immer eine reduzierte ist, wenn dieser Begriff auf Formen mit gebrochenen oder irrationalen reellen Koeffizienten übertragen wird.

Sind nun α, β, γ, δ vier bestimmte ganze Zahlen, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, und setzt man

$$\omega_0 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \omega = \frac{-\gamma + \alpha\omega_0}{\delta - \beta\omega_0},$$

so entspricht, wie man leicht erkennt, dem Hauptfelde (ω_0) ein Feld (ω), welches von drei Kreisbogen begrenzt wird, deren Mittelpunkte stets in der Abszissenachse liegen, und welche in gerade Linien ausarten können; die den Eckpunkten

$$\varrho, \quad -\varrho^2, \quad \infty$$

des Hauptfeldes entsprechenden Eckpunkte des Feldes (ω) sind

$$\frac{-\gamma+\alpha\varrho}{\delta-\beta\varrho}, \quad \frac{-\gamma-\alpha\varrho^2}{\delta+\beta\varrho^2}, \quad \frac{-\alpha}{\beta},$$

deren letzter der Klasse R angehört. Offenbar entspricht den vier Zahlen $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ dasselbe Feld (ω); sonst aber entsprechen, wie die genaue Untersuchung zeigt, zwei verschiedenen Systemen von vier Zahlen α, β, γ, δ immer zwei verschiedene Felder (ω), welche ganz außerhalb einander liegen und höchstens eine Grenzlinie oder auch nur einen Eckpunkt gemeinsam haben können. Die ganze Halbebene S einschließlich R besteht aus unendlich vielen solchen, den verschiedenen Systemen oder Substitutionen $\pm\alpha$, $\pm\beta$, $\pm\gamma$, $\pm\delta$ entsprechenden Kreisbogendreiecken (ω), welche sich in unendlicher Anzahl und Verkleinerung an die Abszissenachse andrängen.

Niemals enthält aber ein solches Feld (ω) einen irrationalen reellen Wert, und in diesem Sinne sage ich, daß bei unserer Untersuchung die Klasse R der rationalen Zahlen die vollständige Begrenzung des Gebiets S bildet. Ist r eine bestimmte rationale Zahl, so gibt es unendlich viele Felder (ω), welche diesen Wert r gemeinschaftlich haben (vgl. § 4, III); das aus allen diesen Feldern bestehende Gebiet $G(r)$ ist durch unendlich viele solche Kreisbogen begrenzt, welche der Linie (3) entsprechen. Ist nun x ein konstanter reeller, aber irrationaler Wert, und nimmt y von $+\infty$ bis 0 ab, so durchläuft $\omega = x + yi$ unendlich viele solche Gebilde $G(r)$, und die Zahlen r, deren Nenner immer größer werden, nähern sich dem Werte x unendlich an. Solange ω einem und demselben Gebiete $G(r)$ angehört, beschreibt die äquivalente Zahl ω_0 im Hauptfelde Kreisbogen, welche immer nach einer bestimmten der beiden Linien (1), (2) hinführen, von hier zu dem symmetrischen Punkte springen und sich durch Verschiebung zu einem einzigen Kreise zusammensetzen lassen; endlich aber muß ein letzter solcher Kreisbogen in die Linie (3) führen; dann tritt ω in das folgende Gebiet $G(r')$, und nun beginnt ω_0 von dem symmetrischen Punkte der Linie (3) aus, eine neue Kreisbogenbewegung in (ω_0), welche dem Durchgange der Variablen ω durch eine endliche Anzahl von Feldern des Gebietes $G(r')$ entspricht (vgl. den Schluß von § 6). Die Annäherung der Zahlen r, r' ... an den Wert x ist nicht ohne Interesse, und ich verspreche mir (viel-

leicht mit Unrecht) von der näheren Untersuchung derselben noch ein brauchbares Resultat, wenigstens für den Fall, daß x die Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten ist.

§ 3.

Die Valenz.

Nach diesen Vorbereitungen gehe ich zu dem Fundamentalsatze meiner Untersuchung über, welcher folgendermaßen lautet:

Es gibt eine Funktion v der Variablen ω im Gebiete S und auf dessen Begrenzung R, welche für alle äquivalenten Werte ω Einen bestimmten Wert besitzt, und zwar so, daß umgekehrt Jedem Werte der unbeschränkten komplexen Variablen v Eine bestimmte Klasse von äquivalenten Werten ω entspricht.

Der Beweis ergibt sich aus den Prinzipien von Riemann (Art. 21 der Inaugural-Dissertation). Man bilde die eine der beiden symmetrischen Hälften des Hauptfeldes (ω_0) auf einer der beiden Hälften der v-Ebene ab, in welche dieselbe durch die Achse der reellen v zerfällt; hierbei bleiben drei reelle Konstanten willkürlich, da zu einem inneren und zu einem Begrenzungspunkte des Orginals die entsprechenden Bildpunkte willkürlich gewählt werden dürfen. Hierauf setze man die Abbildung durch die Symmetrieachse des Feldes (ω_0) hindurch in die andere Hälfte in der Weise fort, daß je zwei zur Achse symmetrischen Punkten ω_0 zwei konjugierte komplexe Werte v entsprechen; hiermit ist das ganze Feld (ω_0) so auf der ganzen v-Ebene abgebildet, daß je zwei äquivalenten Werten ω_0, d. h. je zwei symmetrischen Punkten der Begrenzung von (ω_0) ein und derselbe (reelle) Wert v entspricht; je zwei nicht-äquivalenten Werten ω_0 entsprechen zwei verschiedene Werte v, und umgekehrt entspricht jedem Werte v ein einziger Wert ω_0, oder es entsprechen ihm zwei äquivalente Werte ω_0, welche der Begrenzung von (ω_0) angehören. Man kann daher die Abbildung von (ω_0) auf alle Felder (ω) der ganzen Halbebene S und deren Begrenzung R so ausdehnen, daß je zwei äquivalenten Werten ω ein und derselbe Wert v entspricht, und es leuchtet ein, daß bei dem Übergange von einem Felde (ω) durch die Begrenzung desselben zu einem benachbarten Felde die Funktion v sich stetig ändert.

Sind nun A, B, C, D beliebige reelle Konstanten, so hat die Funktion

$$\frac{C+Dv}{A+Bv}$$

dieselben Eigenschaften wie v, und sie nimmt ebenfalls jeden reellen Wert einmal an, wenn ω_0 die ganze Begrenzung der einen symmetrischen Hälfte des Feldes (ω_0) durchläuft; die drei verfügbaren Konstanten sollen nun so gewählt werden, daß

$$\begin{array}{llll} \text{dem Werte } \omega_0 = \varrho & \text{der Wert} & v = 0, \\ \text{„ „ } \omega_0 = i & \text{„ „} & v = 1, \\ \text{„ „ } \omega_0 = \infty & \text{„ „} & v = \infty \end{array}$$

entspricht. Die hierdurch bestimmte Funktion v will ich die Valenz von ω nennen und mit $\mathrm{val}(\omega)$ bezeichnen. Äquivalente Zahlen ω sind demnach Zahlen von gleicher Valenz.

§ 4.

Windungspunkte.

Um von dieser Definition der Funktion v zu ihrer analytischen Bestimmung zu gelangen, betrachten wir zunächst die umgekehrte Funktion; ist ω ein Zweig derselben, so ist jeder andere von der Form

$$\omega_1 = \frac{\gamma+\delta\omega}{\alpha+\beta\omega},$$

wo α, β, γ, δ vier ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta-\beta\gamma=1$ genügen, und es fragt sich, ob zwei solche im allgemeinen verschiedene Zweige in einem Windungspunkte v, für welchen $\omega=\omega_1=\tau$ wird, zusammenhängen können. Hierzu ist erforderlich, daß τ eine Wurzel der Gleichung

$$\beta\tau^2+(\alpha-\delta)\tau-\gamma=0,$$

also

$$(2\beta\tau+\alpha-\delta)^2=(\alpha+\delta)^2-4$$

ist, und da τ entweder rational ist oder eine positive Ordinate hat, so sind nur folgende drei Fälle möglich:

(I) $$\alpha+\delta=0.$$

Da $\alpha^2+1=(\alpha+i)(\alpha-i)=-\beta\gamma$ ist, und β positiv angenommen werden darf, so ergibt sich aus der Theorie der ganzen komplexen Zahlen von Gauß mit Leichtigkeit, daß man

$$-\alpha+i=(\alpha'-\beta' i)(\gamma'+\delta' i); \qquad \gamma=-(\gamma'+\delta' i)(\gamma'-\delta' i),$$
$$\beta=(\alpha'+\beta' i)(\alpha'-\beta' i); \quad \alpha+i=-(\alpha'+\beta' i)(\gamma'-\delta' i)$$

setzen kann, wo α', β', γ', δ' vier ganze rationale Zahlen bedeuten, welche offenbar der Bedingung $\alpha'\delta' - \beta'\gamma' = 1$ genügen müssen; die ganzen komplexen Zahlen $\alpha' + \beta' i$, $\gamma' + \delta' i$ sind relative Primzahlen, und man erhält

$$\tau = \frac{-\alpha + i}{\beta} = \frac{\gamma}{\alpha + i} = \frac{\gamma' + \delta' i}{\alpha' + \beta' i},$$

d. h. τ ist äquivalent mit i, und folglich ist $v = 1$. Nimmt man nun z. B. $\tau = i$, so ist

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

und die beiden in Rede stehenden Zweige sind

$$\omega_0 \quad \text{und} \quad \frac{-1}{\omega_0}.$$

Diese hängen aber wirklich an der Stelle $v = 1$, $\omega = i$ zusammen; denn wenn v, von Werten mit positiver Ordinate ausgehend, einen positiven Umlauf um $v = 1$ macht, also die Achse der reellen v zuerst zwischen 0 und 1, und nachher zwischen 1 und $+\infty$ kreuzt, so geht ω_0 aus derjenigen Hälfte des Hauptfeldes (ω_0), in welcher die Abszissen negativ sind, durch den Kreisbogen (3) zwischen ϱ und i zunächst in die Hälfte des Feldes $\left(\frac{-1}{\omega_0}\right)$ über, in welcher die Abszissen negativ sind, und dann durch die Ordinatenachse hindurch in die andere Hälfte desselben Feldes $\left(\frac{-1}{\omega_0}\right)$, in welcher die Abszissen positiv sind. Hieraus ergibt sich, daß $(1 - v)$ unendlich klein wie $(\omega - i)^2$ wird, und folglich bleibt in diesem Windungspunkte das Produkt

$$(1 - v)^{-1/2} \frac{dv}{d\omega}$$

endlich und von Null verschieden. Dasselbe gilt für je zwei Zweige

$$\omega = \frac{\gamma' + \delta'\omega_0}{\alpha' + \beta'\omega_0} \quad \text{und} \quad \omega_1 = \frac{-\delta' + \gamma'\omega_0}{-\beta' + \alpha'\omega_0},$$

welche sich für $v = 1$ in irgend einem mit i äquivalenten Werte

$$\tau = \frac{\gamma' + \delta' i}{\alpha' + \beta' i}$$

vereinigen, und zwischen welchen die Relation

$$\omega_1 = \frac{\gamma - \alpha\omega}{\alpha + \beta\omega} = \frac{-(\gamma'^2 + \delta'^2) + (\alpha'\gamma' + \beta'\delta')\omega}{-(\alpha'\gamma' + \beta'\delta') + (\alpha'^2 + \beta'^2)\omega}$$

besteht.

(II) $$\alpha + \delta = \pm 1.$$

Setzt man zur Abkürzung

$$\varepsilon = \frac{1 - \alpha + \delta}{2},$$

so ist, je nachdem das obere oder untere Zeichen gilt,

$$\varepsilon = 1 - \alpha = \delta \quad \text{oder} \quad \varepsilon = -\alpha = 1 + \delta.$$

folglich in beiden Fällen

$$(\varepsilon + \alpha - 1)(\varepsilon + \alpha) = 0,$$

also

$$\alpha\delta = \alpha(2\varepsilon + \alpha - 1) = \varepsilon - \varepsilon^2;$$

mithin ist

$$-\beta\gamma = \varepsilon^2 - \varepsilon + 1 = (\varepsilon + \varrho)(\varepsilon + \varrho^2),$$

und da β positiv angenommen werden darf, so ergibt sich hieraus zufolge der Theorie der aus ϱ gebildeten ganzen komplexen Zahlen, daß man

$$\varepsilon + \varrho = (\alpha' + \beta'\varrho^2)(\gamma' + \delta'\varrho); \qquad \gamma = -(\gamma' + \delta'\varrho)(\gamma' + \delta'\varrho^2),$$
$$\beta = (\alpha' + \beta'\varrho)(\alpha' + \beta'\varrho^2); \quad \varepsilon + \varrho^2 = (\alpha' + \beta'\varrho)(\gamma' + \delta'\varrho^2)$$

setzen kann, wo α', β', γ', δ' vier ganze rationale Zahlen bedeuten, welche offenbar der Bedingung $\alpha'\delta' - \beta'\gamma' = 1$ genügen müssen; die ganzen komplexen Zahlen $\alpha' + \beta'\varrho$, $\gamma' + \delta'\varrho$ sind relative Primzahlen, und man erhält

$$\tau = \frac{\varepsilon + \varrho}{\beta} = \frac{-\gamma}{\varepsilon + \varrho^2} = \frac{\gamma' + \delta'\varrho}{\alpha' + \beta'\varrho},$$

d. h. τ ist äquivalent mit ϱ, und folglich ist $v = 0$. Nimmt man nun z. B. $\tau = \varrho$, so ist $\varepsilon = 0$, $\beta = 1$, also entweder

$$\alpha = 1, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

oder

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = -1,$$

und in der Tat geht, wenn v aus einem Werte mit positiver Ordinate einen positiven Umlauf um $v = 0$ macht, von den drei Zweigen

$$\omega_0, \quad \frac{-1 - \omega_0}{\omega_0}, \quad \frac{-1}{1 + \omega_0}$$

der erste in den zweiten, dieser in den dritten, und dieser wieder in den ersten über. (Macht v denselben Umlauf aus einem Werte mit negativer Ordinate, so gehen die drei Zweige

$$\frac{-1}{\omega_0}, \quad -1 + \omega_0, \quad \frac{-\omega_0}{-1 + \omega_0},$$

welche ebenfalls den Eckpunkt ϱ gemeinschaftlich haben, zyklisch ineinander über.) Hieraus folgt, daß in diesem Windungspunkte das Produkt

$$v^{-2/3}\frac{dv}{d\omega}$$

endlich und von Null verschieden bleibt. Ähnlich verhält es sich für alle anderen mit ϱ äquivalenten Werte τ.

(III) $$(\alpha+\delta)^2 = 4.$$

In diesem und nur in diesem Falle wird τ rational, also ein Repräsentant der Begrenzung R, und folglich wird $v = \infty$. Setzt man (was erlaubt ist) $\alpha + \delta = +2$, und

$$\tau = \frac{1-\alpha}{\beta} = \frac{-\gamma}{1-\alpha} = \frac{m}{n},$$

wo m, n relative Primzahlen, so ergibt sich

$$\alpha = 1 + g\,m\,n, \quad \beta = -g\,n^2, \quad \gamma = +g\,m^2, \quad \delta = 1 - g\,m\,n,$$

wo g eine willkürliche ganze Zahl bedeutet. Nimmt man z. B. $m = 1$, $n = 0$, also $\tau = \infty$, so erkennt man leicht, daß jeder der unendlich vielen Zweige $(g + \omega_0)$ durch einen positiven Umlauf von v um $v = \infty$ in den folgenden Zweig $(g + 1 + \omega_0)$ übergeht. Für unendlich große Werte von ω ist daher die unendlich kleine Größe

$$q^2 = 1^\omega$$

eine einändrige Funktion von v, und da umgekehrt v überall eine einwertige Funktion von 1^ω ist, so bleibt für $\omega = \infty$ das Produkt

$$v\,1^\omega$$

endlich und von Null verschieden, und zugleich wird

$$v^{-1}\frac{dv}{d\omega} = \frac{d\log v}{d\omega} = -2\pi i.$$

Hieraus läßt sich leicht das Verhalten von v für alle anderen rationalen Werte $\omega = \frac{m}{n}$ ableiten.

§ 5.

Differentialgleichungen.

Bedeuten u, v zwei beliebige voneinander abhängige Variable, so wollen wir zur Abkürzung den Differentialausdruck dritter Ordnung

(1) $$\frac{-4}{\sqrt{\frac{dv}{du}}}\frac{d}{dv}\frac{d}{dv}\sqrt{\frac{dv}{du}} = [v, u]$$

setzen; man findet leicht, daß derselbe die beiden Eigenschaften

$$[u, v] = -[v, u]\left(\frac{dv}{du}\right)^2, \tag{2}$$

$$[v, u]\,dv^2 + [w, v]\,dw^2 + [u, w]\,du^2 = 0 \tag{3}$$

besitzt, wo w ebenfalls eine beliebige Funktion von u, also auch von v bedeutet. Sind ferner u, w kollineare Variable, womit ausgedrückt sein soll, daß

$$w = \frac{C + Du}{A + Bu} \tag{4}$$

ist, wo A, B, C, D Konstanten bedeuten, so ist

$$[u, w] = [w, u] = 0, \tag{5}$$

und folglich, was auch v sein mag,

$$[v, u] = [v, w]; \tag{6}$$

und umgekehrt, wenn $[u, w] = 0$ ist, so sind u, w kollinear, d. h. die Gleichung (4) ist das allgemeine Integral der Differentialgleichung (5).

Diese allgemeinen Sätze wenden wir auf folgendes Beispiel an. Es sei wieder $v = \mathrm{val}(\omega)$, so ist offenbar

$$[v, \omega] = f(\omega)$$

eine einwertige Funktion von ω, da sie auf rationale Weise aus den Derivierten erster, zweiter und dritter Ordnung von v in bezug auf ω gebildet ist; wir wollen nun beweisen, daß sie auch eine einwertige Funktion von v ist. In der Tat, setzt man $v_1 = \mathrm{val}(\omega_1)$, wo ω_1 eine neue Variable bedeutet, so ist $f(\omega_1) = [v_1, \omega_1]$; und wenn ω_1 mit ω durch die Gleichung

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

verbunden wird, wo α, β, γ, δ ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, so ist $v_1 = v$, also $f(\omega_1) = [v, \omega_1]$; da außerdem ω, ω_1 kollinear sind, so folgt aus (6), daß $[v, \omega] = [v, \omega_1]$, also $f(\omega) = f(\omega_1)$ ist; mithin entspricht jedem Werte v nur ein einziger Wert $f(\omega)$. Wir können daher

$$[v, \omega] = F(v) \tag{7}$$

setzen, wo $F(v)$ eine einwertige Funktion von v bedeutet. Aus ihrer Bildung geht hervor, daß sie für alle Werte v, mit Ausnahme von 1, 0, ∞ endlich bleibt, und da für diese Werte von v, denen man

die Werte i, ϱ, ∞ von ω entsprechen lassen darf, respektive das Produkt

$$(1-v)^{-1/2}\frac{dv}{d\omega},\quad v^{-2/3}\frac{dv}{d\omega},\quad v^{-1}\frac{dv}{d\omega}$$

endlich und von Null verschieden bleibt, so ergibt sich, daß entsprechend

$$(1-v)^2F(v)=\tfrac{3}{4},\quad v^2F(v)=\tfrac{8}{9},\quad v^2F(v)=1$$

wird; da folglich die einwertige Funktion $v^2(1-v)^2F(v)$ für alle endlichen Werte von v endlich bleibt und für $v=\infty$ unendlich groß von zweiter Ordnung wird, so ist sie eine ganze Funktion zweiten Grades, deren Koeffizienten aus den vorstehenden drei Gleichungen sich unmittelbar ergeben; auf diese Weise findet man

$$(8)\qquad \begin{cases} F(v)=\dfrac{36v^2-41v+32}{36v^2(1-v)^2} \\ \qquad =\dfrac{8}{9v^2}+\dfrac{23}{36v}+\dfrac{3}{4(1-v)^2}+\dfrac{23}{36(1-v)}. \end{cases}$$

Die Funktion $v=\mathrm{val}(\omega)$ ist daher eine Lösung v' der Differentialgleichung dritter Ordnung

$$(9)\qquad [v'\,\omega]=F(v');$$

um ihr allgemeines Integral v' zu finden, setze man $v'=\mathrm{val}(\omega')$, wo ω' eine neue Variable bedeutet; dann ist $[v',\omega']=F(v')$, also $[v',\omega']=[v',\omega]$, woraus mit Rücksicht auf (2) und (3) folgt, daß $[\omega,\omega']=0$, also

$$(10)\qquad \omega'=\frac{C+D\omega}{A+B\omega},\quad v'=\mathrm{val}\left(\frac{C+D\omega}{A+B\omega}\right)$$

ist, wo A, B, C, D willkürliche Konstanten bedeuten. Zugleich ergibt sich aus (3), daß das System der beiden Gleichungen

$$(11)\qquad v=\mathrm{val}(\omega),\quad v'=\mathrm{val}\left(\frac{C+D\omega}{A+B\omega}\right)$$

das allgemeine Integral der Differentialgleichung dritter Ordnung

$$(12)\qquad [v,v']\,dv^2=F(v)\,dv^2-F(v')\,dv'^2$$

bildet (vgl. Fund. nova §§ 32, 33).

§ 6.

Die elliptischen Modulfunktionen.

Aus der Bildung des Ausdrucks $[v,\omega]$ geht hervor, daß $\sqrt{\frac{dv}{d\omega}}$ einer linearen Differentialgleichung zweiter Ordnung in bezug auf v genügt; allein es ist offenbar zweckmäßiger, die Größe

$$(1)\qquad w=const\,v^{-1/2}(1-v)^{-1/4}\left(\frac{dv}{d\omega}\right)^{1/2}$$

einzuführen, welche für alle Werte von ω innerhalb S endlich und von Null verschieden bleibt, während sie in der Begrenzung R stets unendlich klein wird; mithin ist $\log w$ und jede Potenz von w, sobald ihr Wert an einer Stelle des einfach zusammenhängenden Gebietes S gegeben ist, eine völlig bestimmte, durchaus einwertige Funktion von ω. Aus der obigen Differentialgleichung dritter Ordnung (7) in § 5 folgt nun, daß w der hypergeometrischen Differentialgleichung

$$v(1-v)\frac{d^2w}{dv^2} + (\tfrac{2}{3} - \tfrac{7}{6}v)\frac{dw}{dv} - \tfrac{1}{144}w = 0 \tag{2}$$

genügt, deren allgemeines Integral $(const + const\,\omega)w$ in der Form

$$const \cdot F(\tfrac{1}{12}, \tfrac{1}{12}, \tfrac{2}{3}, v) + const \cdot F(\tfrac{1}{12}, \tfrac{1}{12}, \tfrac{1}{2}, 1-v)$$

enthalten ist, wo F die Reihe von Gauß bedeutet. Dasselbe hätte man auch durch direkte Untersuchung der Größe w als einer Riemannschen P-Funktion erhalten, und noch einfacher würde man, wie mein Freund Heinrich Weber in Königsberg mir vor einem Jahre mitgeteilt hat, durch die Betrachtungen zum Ziele gelangen können, welche den Gegenstand der Abhandlung XXV in Riemanns Werken bilden. Endlich bemerke ich, daß das in § 3 behandelte Abbildungsproblem sich auch durch die Untersuchungen von Weierstrass und Schwarz erledigen läßt.

Von besonderem Interesse ist nun die Quadratwurzel der Größe w, und ich will dieselbe durch

$$\eta(\omega) = const\, v^{-1/6}(1-v)^{-1/6}\left(\frac{dv}{d\omega}\right)^{1/4} \tag{3}$$

bezeichnen; sie ist, wie schon bemerkt, eine einwertige Funktion von ω, welche für alle Werte von ω innerhalb S endlich und von Null verschieden bleibt; für $\omega = \infty$ wird sie unendlich klein wie $v^{-1/24}$, also wie $1^{\omega/24}$; ich wähle die Konstante so, daß für $\omega = \infty$ das Produkt

$$1^{-\frac{\omega}{24}}\eta(\omega) = 1 \tag{4}$$

wird, und hierdurch ist $\eta(\omega)$ für das ganze Gebiet S vollständig bestimmt. Bedeuten α, β, γ, δ wieder vier ganze Zahlen, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, so folgt aus

$$\mathrm{val}\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \mathrm{val}(\omega)$$

die Eigenschaft

$$\eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = c(\alpha + \beta\omega)^{1/2}\eta(\omega), \tag{5}$$

wo $c^{24} = 1$ ist; speziell ergibt sich leicht

$$(6) \qquad \eta(1+\omega) = 1^{1/24}\,\eta(\omega); \quad \eta\left(\frac{-1}{\omega}\right) = 1^{-1/8}\,\omega^{1/2}\,\eta(\omega),$$

wo $\omega^{1/2} = 1^{1/8}$ wird, wenn $\omega = 1^{1/4} = i$ ist. Die Funktion ist durch die genannten Eigenschaften vollständig bestimmt; denn wenn $f(\omega)$ ebenso beschaffen ist, so ist der Quotient $f(\omega) : \eta(\omega)$ zufolge (6) eine einwertige Funktion von $v = \mathrm{val}(\omega)$, welche für alle endlichen Werte von v endlich bleibt und zufolge (4) für $v = \infty$ den Wert Eins annimmt, und folglich $const = 1$ ist.

Um nun den Zusammenhang zwischen dieser Funktion $\eta(\omega)$ und dem Modul der elliptischen Integrale oder dessen Quadrat k herzustellen, betrachte ich die der Transformation zweiter Ordnung entsprechenden Funktionen

$$(7) \qquad \eta_1(\omega) = \eta(2\omega); \quad \eta_2(\omega) = \eta\left(\frac{\omega}{2}\right); \quad \eta_3(\omega) = \eta\left(\frac{1+\omega}{2}\right),$$

welche folgende Eigenschaften besitzen. Aus (6) folgt

$$\eta_1(1+\omega) = 1^{1/12}\,\eta_1(\omega); \quad \eta_1\left(\frac{-1}{\omega}\right) = 1^{-1/8}\left(\frac{\omega}{2}\right)^{1/2}\eta_2(\omega),$$

$$\eta_2(1+\omega) = \eta_3(\omega) \quad ; \quad \eta_2\left(\frac{-1}{\omega}\right) = 1^{-1/8}\,(2\omega)^{1/2}\,\eta_1(\omega),$$

$$\eta_3(1+\omega) = 1^{1/24}\,\eta_2(\omega); \quad \eta_3\left(\frac{-1}{\omega}\right) = 1^{-1/8}\,\omega^{1/2}\,\eta_3(\omega),$$

und für $\omega = \infty$ folgt aus (4)

$$1^{-\frac{\omega}{12}}\eta_1(\omega) = 1; \quad 1^{-\frac{\omega}{48}}\eta_2(\omega) = 1; \quad 1^{-\frac{\omega}{48}}\eta_3(\omega) = 1^{1/48}.$$

Hieraus ergibt sich, daß die Funktion

$$f(\omega) = \frac{\eta_1(\omega)\,\eta_2(\omega)\,\eta_3(\omega)}{\eta(\omega)^3}$$

die Eigenschaften

$$f(1+\omega) = f(\omega), \quad f\left(\frac{-1}{\omega}\right) = f(\omega)$$

besitzt und folglich eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist, weil alle Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ sich aus den beiden Substitutionen $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ und $\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$ zusammensetzen lassen; sie bleibt vermöge ihrer Definition endlich für alle endlichen Werte v und wird $= 1^{1/48}$ für $\omega = \infty$, $v = \infty$, folglich ist sie eine Konstante. Es ist daher

$$(8) \qquad \eta_1(\omega)\,\eta_2(\omega)\,\eta_3(\omega) = 1^{1/48}\,\eta(\omega)^3,$$

und ein ähnlicher Satz gilt für Transformationen von beliebiger Ordnung. Ebenso ergibt sich, daß die Funktion

$$f_1(\omega) = \frac{2^4\,\eta_1(\omega)^8 + \eta_2(\omega)^8 + 1^{1/3}\,\eta_3(\omega)^8}{\eta(\omega)^8}$$

die Eigenschaften

$$f_1(1+\omega) = 1^{1/3} f_1(\omega), \quad f_1\left(\frac{-1}{\omega}\right) = f_1(\omega)$$

besitzt, woraus folgt, daß $f_1(\omega)^3$ eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist, welche für jeden endlichen Wert von v endlich ist; für $\omega = \infty$, $v = \infty$ wird ferner $f_1(\omega)\,1^{\omega/6} = 0$, also auch $f_1(\omega)^3 v^{-1/2} = 0$; also kann $f_1(\omega)^3$ nicht einmal von der Ordnung $v^{1/2}$ unendlich groß werden, und folglich ist $f_1(\omega)^3$, also auch $f_1(\omega)$ eine Konstante, und zwar $= 0$, wie sich aus $f_1(1+\omega) = 1^{1/3} f_1(\omega)$ ergibt. Es ist daher

$$2^4\,\eta_1(\omega)^8 + \eta_2(\omega)^8 + 1^{1/3}\,\eta_3(\omega)^8 = 0. \tag{9}$$

Führt man nun die folgenden Bezeichnungen ein (welche mit denen von Hermite übereinstimmen)

$$\begin{cases} \varphi(\omega) = 1^{1/48}\sqrt{2}\cdot\dfrac{\eta_1(\omega)}{\eta_3(\omega)} = \sqrt[4]{\varkappa} = \sqrt[8]{k}, \\ \psi(\omega) = 1^{1/48}\dfrac{\eta_2(\omega)}{\eta_3(\omega)} = \sqrt[4]{\varkappa'} = \varphi\left(\dfrac{-1}{\omega}\right), \\ \chi(\omega) = 1^{1/48}\sqrt[6]{2}\cdot\dfrac{\eta(\omega)}{\eta_3(\omega)}, \end{cases} \tag{10}$$

so folgt aus (9)

$$\varphi(\omega^8) + \psi(\omega)^8 = 1, \quad \varkappa^2 + \varkappa'^2 = 1 \tag{11}$$

und aus (8)

$$\varphi(\omega)\,\psi(\omega) = \chi(\omega)^3; \tag{12}$$

außerdem kann man die Größen K, K' durch die Gleichungen

$$\sqrt{\frac{2K}{\pi}} = 1^{-1/24}\,\frac{\eta_3(\omega)^2}{\eta(\omega)}, \quad K'i = K\omega \tag{13}$$

definieren.

Für die Funktion $k = \varkappa^2 = \varphi(\omega)^8$ ergeben sich nun aus dem Obigen die Eigenschaften

$$\varphi(1+\omega)^8 = -2^4\,\frac{\eta_1(\omega)^8}{\eta_2(\omega)^8} = \frac{k}{k-1} \tag{14}$$

$$\varphi\left(\frac{-1}{\omega}\right)^8 = 1^{1/6}\,\frac{\eta_2(\omega)^8}{\eta_3(\omega)^8} = \varkappa'^2 = 1-k, \tag{15}$$

und außerdem ist

$$k\,1^{-\frac{\omega}{2}} = 2^4 \quad \text{für} \quad \omega = \infty. \tag{16}$$

Hieraus folgt, daß die Funktion

$$f_2(\omega) = \frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2}$$

die Eigenschaften

$$f_2(1+\omega) = f_2(\omega), \quad f_2\left(\frac{-1}{\omega}\right) = f_2(\omega)$$

besitzt, mithin eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist; sie kann nur dann unendlich werden, wenn $k = 0,\ 1,\ \infty$ wird; da aber k und $(1-k)$ Quotienten von η-Funktionen sind, so kann dies nur dann geschehen, wenn $v = \infty$ wird, also z. B. für $\omega = \infty$; in diesem Fall wird aber k zufolge (16) unendlich klein wie $1^{\omega/2}$, also wie $v^{-1/2}$, und folglich $f_2(\omega)$ unendlich groß wie v; mithin ist $f_2(\omega)$ eine ganze Funktion ersten Grades von v, also

$$\frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2} = av + b.$$

Um die Konstante b zu bestimmen, setze man $\omega = \varrho$, also $v = 0$; da nun

$$\eta_3(\varrho) = \eta\left(\frac{1+\varrho}{2}\right) = \eta\left(\frac{-1}{2\varrho}\right),$$

und folglich

$$\eta_3(\varrho)^8 = \eta\left(\frac{-1}{2\varrho}\right)^8 = (2\varrho)^4\,\eta(2\varrho)^8 = (2\varrho)^4\,\eta_1(\varrho)^8$$

ist, so ergibt sich für k der Wert

$$\varphi(\varrho)^8 = 1^{1/6}\,2^4\frac{\eta_1(\varrho)^8}{\eta_3(\varrho)^8} = -\varrho, \tag{17}$$

und folglich ist $b = 0$. Um a zu bestimmen, setze man $\omega = i$, also $v = 1$; dann ergibt sich für k der Wert

$$\varphi(i)^8 = \varphi\left(\frac{-1}{i}\right)^8 = 1 - \varphi(i)^8 = \tfrac{1}{2}, \tag{18}$$

woraus $a = \frac{27}{4}$ folgt. Auf diese Weise erhalten wir das Resultat

$$v = \mathrm{val}(\omega) = \tfrac{4}{27}\frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2}. \tag{19}$$

In dieser Form erscheint die Funktion v an mehreren Stellen der berühmten Abhandlung von Hermite über die Theorie der Modulargleichungen; ich bemerke zugleich, daß auch Gauß (Werke III, S. 386) die Absicht gehabt hat, eine solche Funktion einzuführen.

Man kann, in ähnlicher Weise, wie dies oben für $\eta(\omega)$ geschehen ist, beweisen, daß die Funktion $k = \varphi(\omega)^8$ durch die an-

gegebenen Eigenschaften vollständig bestimmt ist; die Prinzipien, auf welche sich der Nachweis der Existenz der Funktion v gestützt hat, führen auch ebenso leicht zur unmittelbaren Bestimmung der Funktion k; dieselbe erfordert, wie aus der Kombination von (14) und (15) hervorgeht, zu ihrer vollen Ausbreitung im Gebiete S sechs ganze oder zwölf halbe Felder (ω), welche letzteren so gewählt werden können, daß sie symmetrisch zu beiden Seiten der rein imaginären ω liegen. Man erhält auf diese Weise die Differentialgleichung dritter Ordnung

$$[k, \omega] = \frac{(k+\varrho)(k+\varrho^2)}{k^2(1-k)^2}, \tag{20}$$

und ebenso, wie wir oben zu einer linearen Differentialgleichung zweiter Ordnung für $w = const \cdot \eta(\omega)^2$ gelangt sind, ergibt sich hier, wenn man

$$\frac{dk}{d\omega} = \frac{-4}{\pi i} k(1-k)K^2 \tag{21}$$

setzt, die bekannte lineare Differentialgleichung

$$\frac{d}{dk}\left(k(1-k)\frac{dK}{dk}\right) = \tfrac{1}{4}K, \tag{22}$$

welche den Ausgangspunkt der Abhandlung von Fuchs bildet. Natürlich würde man dieselben Resultate auch aus dem Zusammenhang zwischen k und v finden, welcher in (19) ausgedrückt ist.

Da k durch die obigen Eigenschaften als Funktion von ω vollständig bestimmt ist, und da die in der Theorie der elliptischen oder ϑ-Funktionen auftretende Funktion

$$\frac{\vartheta_2(0,\omega)^4}{\vartheta_3(0,\omega)^4}$$

wirklich dieselben Eigenschaften besitzt, so ergibt sich aus dieser Identität beider Funktionen leicht, daß

$$\begin{cases} \vartheta(0,\omega) = \dfrac{\eta_2(\omega)^2}{\eta(\omega)}; \quad \vartheta_1'(0,\omega) = 2\pi\eta(\omega)^3, \\ \vartheta_2(0,\omega) = 2\dfrac{\eta_1(\omega)^2}{\eta(\omega)}; \quad \vartheta_3(0,\omega) = 1^{-\frac{1}{24}}\dfrac{\eta_3(\omega)^2}{\eta(\omega)}, \end{cases} \tag{23}$$

und folglich

$$\eta(\omega) = 1^{\omega/24}\Pi(1-1^{\omega\nu}) = q^{1/12}\Pi(1-q^{2\nu}) \tag{24}$$

ist, wo ν alle positiven ganzen Zahlen durchläuft und

$$q = 1^{\omega/2} \tag{25}$$

gesetzt ist. Allein es ist mir bisher nicht geglückt, diese Darstellung von $\eta(\omega)$ als explizite Funktion von ω lediglich aus ihrer obigen Definition, also ohne die Hilfe der Theorie der ϑ-Funktionen abzuleiten.

Die eingehende Beschäftigung mit dieser Funktion $\eta(\omega)$, zu welcher mich zuerst die Untersuchung über die Anzahl der Idealklassen in kubischen Körpern veranlaßt hatte, ist mir später von großem Nutzen bei der Bearbeitung des zweiten Fragmentes XXVII aus dem Nachlasse von Riemann gewesen. Die Zahlen (m, n), auf welche ich durch das Studium desselben geführt bin, besitzen in der Tat sehr interessante Eigenschaften; ist z. B. n eine positive ungerade Zahl, und m relative Primzahl zu n, so ist

$$\left(\frac{m}{n}\right) \equiv \frac{n+1}{2} - (m, n) \pmod 4,$$

wo $\left(\frac{m}{n}\right)$ das Zeichen von Legendre und Jacobi aus der Theorie der quadratischen Reste bedeutet; ist m ebenfalls positiv und ungerade, so ergibt sich hieraus unter Zuziehung des Satzes

$$2\,m\,(m, n) + 2\,n\,(n, m) = 1 + m^2 + n^2 - 3\,m\,n$$

sofort der verallgemeinerte Reziprozitätssatz in der Form

$$\left(\frac{m}{n}\right) + \left(\frac{n}{m}\right) \equiv 2\left(1 + \frac{m-1}{2} \cdot \frac{n-1}{2}\right) \pmod 4.$$

Ich erlaube mir hier auf eine Stelle der Abhandlung von Fuchs aufmerksam zu machen, in welche, wie mir scheint, sich ein Irrtum eingeschlichen hat. Sind m, n relative Primzahlen, und nähert sich $\omega = x + yi$ dem rationalen Werte $\frac{m}{n}$ so an, daß x konstant $= \frac{m}{n}$ bleibt, und y positiv unendlich klein wird, so nähert sich k, wie aus dem Fragment von Riemann oder auch aus der obigen Theorie folgt, dem Werte

$$\begin{aligned} k &= \infty, \quad \text{wenn} \quad m \equiv 1, \quad n \equiv 1 \pmod 2, \\ k &= 1, \quad \text{„} \quad m \equiv 0, \quad n \equiv 1 \quad \text{„} \\ k &= 0, \quad \text{„} \quad m \equiv 1, \quad n \equiv 0 \quad \text{„} \end{aligned}$$

ist; wenn dagegen $\omega = x + yi$ sich auf dieselbe Weise einem irrationalen reellen Wert x nähert, so ergibt sich aus der obigen Theorie (vgl. den Schluß von § 2), daß k sich keinem bestimmten Werte nähert, sondern unaufhörliche Schwankungen erleidet. Dies steht im Widerspruch mit dem Satze II auf S. 27 der genannten

Abhandlung, in welchem behauptet wird, daß die Größe u ($= k^{-1}$ nach meiner Bezeichnung) sich immer einem der beiden Werte Null oder Eins annähern müsse, und mir scheint, als sei der Beweis dieser Behauptung gerechten Bedenken unterworfen, namentlich in dem Teile, welcher auf die Worte „ou n'y parvînt pas“ (S. 26) folgt. Doch ist diese Abweichung von keiner wesentlichen Bedeutung für den Hauptgegenstand der sehr interessanten Abhandlung.

§ 7.

Transformation.

Ich will nun noch zum Schluß die Theorie der algebraischen Gleichungen zwischen Valenzen begründen, welche den Modulargleichungen in der Theorie der Transformation der elliptischen oder ϑ-Funktionen entsprechen. Es sei wieder $v = \mathrm{val}(\omega)$, und

$$v_n = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right),$$

wo A, B, C, D vier beliebige ganze Zahlen ohne gemeinschaftlichen Teiler und von positiver Determinante

$$AD - BC = n$$

bedeuten. Die Anzahl aller möglichen solchen Funktionen v_n, welche einer gegebenen positiven ganzen Zahl n entsprechen, ist endlich und leicht zu bestimmen. Es sei nämlich, wenn A, B, C, D gegeben sind, ∂ der größte positive gemeinschaftliche Teiler der beiden Zahlen

$$B = \partial\beta, \quad D = \partial\delta,$$

so ist

$$n = a\partial, \quad \text{wo} \quad a = A\delta - C\beta;$$

nun kann man, da β, δ relative Primzahlen sind, die beiden ganzen Zahlen α, γ stets und nur auf eine einzige Art so bestimmen, daß $\alpha\delta - \beta\gamma = 1$ wird, und daß zugleich die Zahl

$$c = C\alpha - A\gamma$$

der Bedingung

$$0 \leqq c < a$$

genügt; dann ist

$$\begin{pmatrix} A, & B \\ C, & D \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix},$$

mithin

$$v_n = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right) = \mathrm{val}\left(\frac{c + \partial\omega}{a}\right),$$

und da A, B, C, D keinen gemeinschaftlichen Teiler haben, so gilt dasselbe auch von den drei Zahlen a, c, ∂. Um daher für eine gegebene Zahl n alle möglichen Funktionen v_n zu erhalten, braucht man nur a alle positiven Divisoren von n durchlaufen zu lassen; für jeden solchen Divisor a bestimmt sich ∂ durch die Gleichung $a\partial = n$; ist nun e der größte gemeinschaftliche Teiler von a und ∂, so darf, wenn $\varphi(e)$ die Anzahl derjenigen Zahlen 0, 1, 2, ... $(e-1)$ bedeutet, welche relative Primzahlen zu e sind, die Zahl c alle diejenigen $\frac{a}{e}\varphi(e)$ Zahlen durchlaufen, welche relative Primzahlen zu e sind und zugleich der Bedingung $0 \leqq c < a$ genügen. Es läßt sich ferner leicht zeigen, daß je zwei verschiedenen Systemen von drei solchen Zahlen a, c, ∂ auch zwei nichtidentische Funktionen

$$v_n = \mathrm{val}\left(\frac{c + \partial\omega}{a}\right)$$

entsprechen, und folglich ist die Anzahl aller wirklich verschiedenen Funktionen v_n gleich

$$\sum \frac{a}{e}\varphi(e) = \psi(n),$$

wo a alle Divisoren von n durchläuft, und e jedesmal die oben angegebene Bedeutung hat. Aus dieser Form folgt sofort, wenn n, n' relative Primzahlen sind, der Satz

$$\psi(nn') = \psi(n)\psi(n');$$

der Fall einer Primzahlpotenz ist leicht zu erledigen, und hieraus ergibt sich allgemein

$$\psi(n) = n\Pi\left(1 + \frac{1}{p}\right),$$

wo p alle verschiedenen in n aufgehenden Primzahlen durchläuft.

Setzt man zur Abkürzung $\psi(n) = \nu$, und bezeichnet mit

$$f_1(\omega),\ f_2(\omega),\ \ldots,\ f_\nu(\omega)$$

die sämtlichen verschiedenen in der Form

$$\mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right)$$

enthaltenen Funktionen v_n, so sind, wenn α, β, γ, δ vier bestimmte ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, auch die ν Funktionen

$$f_1\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right),\quad f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right),\quad \ldots,\ f_\nu\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)$$

voneinander verschieden; da ferner jedes System von vier ganzen Zahlen A, B, C, D ohne gemeinschaftlichen Teiler, welche die Bedingung $AD - BC = n$ befriedigen, durch die Zusammensetzung

$$\begin{pmatrix} A, & B \\ C, & D \end{pmatrix}\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} A', & B' \\ C', & D' \end{pmatrix}$$

wieder ein System von vier ganzen Zahlen A', B', C', D' liefert, welche keinen gemeinschaftlichen Teiler haben und der Bedingung $A'D' - B'C' = n$ genügen, so ist jede dieser Funktionen identisch mit einer der ν Funktionen v_n, und folglich ist ihr Komplex identisch mit dem der Funktionen v_n. Bedeutet daher σ eine willkürliche, von ω unabhängige Größe, so ist das über alle ν Funktionen v_n ausgedehnte Produkt

$$\Pi(\sigma - v_n)$$

eine einwertige Funktion von ω, welche ungeändert bleibt, wenn ω durch eine beliebige äquivalente Größe

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

ersetzt wird, und folglich kann man

$$\Pi(\sigma - v_n) = F_n(\sigma, v)$$

setzen, wo $F_n(\sigma, v)$ eine ganze Funktion ν^{ten} Grades von σ bedeutet, deren Koeffizienten einwertige Funktionen von $v = \text{val}(\omega)$ sind. Ist v endlich, so gehört ω dem Innern des Gebietes S an, und folglich ist jeder der ν Werte v_n, also auch $F_n(\sigma, v)$ endlich. Wird aber $v = \infty$, so darf man annehmen, daß auch $\omega = \infty$ wird; da nun in diesem Falle

$$1^{\omega}\,\text{val}(\omega) = m,$$

also

$$1^{\frac{\partial}{a}\omega}\,\text{val}\left(\frac{c + \partial\omega}{a}\right) = m\,1^{-\frac{c}{a}}$$

wird, wo m endlich und von Null verschieden ist [nämlich $= 2^{-6}3^{-3}$, wie sich aus (16) und (19) in § 6 ergibt], so folgt, daß $F_n(\sigma, v)$ gleichzeitig mit v unendlich groß wird, und zwar von der Ordnung

$$\sum \frac{\partial}{a}\cdot\frac{a}{e}\varphi(e) = \sum \frac{\partial}{e}\varphi(e) = \sum \frac{a}{e}\varphi(e) = \nu;$$

mithin ist

$$F_n(\sigma, v) = \sigma^{\nu} + V_1\sigma^{\nu-1} + V_2\sigma^{\nu-2} + \cdots + V_{\nu}$$

auch eine ganze Funktion ν^{ten} Grades von v, und es ist z. B.

$$-V_1 = \sum v_n = \frac{1}{m^{n-1}}v^n + \cdots$$

eine ganze Funktion n^{ten} Grades von v. Die ν Funktionen v_n sind daher algebraische Funktionen von v, nämlich die Wurzeln der Gleichung

$$F_n(v_n, v) = 0.$$

Diese Valenzgleichung ist irreduktibel. Genügt nämlich die Funktion $v_n' = \text{val}(n\,\omega)$ einer Gleichung von der Form

$$G(v_n', v) = 0,$$

wo $G(\sigma, v)$ eine ganze rationale Funktion der beiden Größen σ, v bedeutet, so ist identisch

$$G(\text{val}(n\,\omega),\ \text{val}(\omega)) = 0,$$

folglich auch, wenn die vier ganzen Zahlen α, β, γ, δ der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen,

$$G\Big(\text{val}\Big(\frac{n\gamma + n\delta\,\omega}{\alpha + \beta\,\omega}\Big),\ \text{val}(\omega)\Big) = 0;$$

läßt sich nun zeigen, wie gleich geschehen soll, daß die Funktion

$$\text{val}\Big(\frac{n\gamma + n\delta\,\omega}{\alpha + \beta\,\omega}\Big)$$

durch geeignete Wahl der vier Zahlen α, β, γ, δ zur Übereinstimmung mit jeder der ν Funktionen

$$v_n = \text{val}\Big(\frac{c + \partial\,\omega}{a}\Big)$$

gebracht werden kann, so genügt jede Funktion v_n der Gleichung $G(v_n, v) = 0$, mithin ist $G(\sigma, v)$ teilbar durch $F_n(\sigma, v)$, woraus die Irreduktibilität dieser letzteren Funktion folgt. Es ist also nur noch zu beweisen, daß, wenn drei Zahlen a, c, ∂ ohne gemeinschaftlichen Teiler gegeben sind, welche der Bedingung $a\,\partial = n$ genügen, man immer acht ganze Zahlen α, β, γ, δ, α', β', γ', δ' so wählen kann, daß $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma' = 1$ und

$$\begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}\begin{pmatrix}a, & 0\\ c, & \partial\end{pmatrix}$$

wird. Die allgemeinste Art, solche Zahlen zu finden, ist die folgende (vgl. die zu Anfang dieses Paragraphen ausgeführte Reduktion). Man wähle für γ eine beliebige Zahl, welche relative Primzahl zu ∂ ist, und setze

$$\delta' = a\,\delta,$$

so kann man γ so wählen, daß die Zahl

$$\gamma' = \partial\,\gamma - c\,\delta$$

relative Primzahl zu δ' wird; denn wie man auch γ wählen mag, so ist γ' jedenfalls unteilbar durch diejenigen Primzahlen, welche gleichzeitig in a und in ∂, also in e aufgehen, weil a, c, ∂ keinen gemeinschaftlichen Teiler haben, und weil δ relative Primzahl zu ∂ ist; bezeichnet man ferner mit p das Produkt aller übrigen in a aufgehenden Primzahlen (oder die Einheit, falls keine solche vorhanden sind), so ist ∂ relative Primzahl zu p, also auch zu $p\delta$, und folglich durchläuft γ' gleichzeitig mit γ ein vollständiges Restsystem (mod. $p\delta$); mithin gibt es unendlich viele Werte von γ, für welche γ' relative Primzahl zu $p\delta$ und folglich auch zu $\delta' = a\delta$ wird. Nachdem δ, γ so gewählt sind, daß δ', γ' relative Primzahlen werden, wähle man eine beliebige Lösung α', β' der Gleichung

$$\alpha'\delta' - \beta'\gamma' = 1,$$

und setze

$$\alpha = a\alpha' + c\beta', \quad \beta = \partial\beta',$$

so wird

$$\alpha\delta - \beta\gamma = (a\alpha' + c\beta')\delta - \partial\beta'\gamma = \alpha'\delta' - \beta'\gamma' = 1,$$

und die gefundenen acht Zahlen erfüllen die obigen Forderungen weil

$$n\gamma = a\gamma' + c\delta', \quad n\delta = \partial\delta'$$

ist.

Die Funktion $F_n(\sigma, v)$ ist symmetrisch in bezug auf σ und v, wenn $n > 1$ ist. Denn aus der Identität

$$F_n(\mathrm{val}(n\omega), \mathrm{val}(\omega)) = 0$$

folgt, wenn man ω durch $\frac{\omega}{n}$ ersetzt, die Gleichung

$$F_n\left(v, \mathrm{val}\left(\frac{\omega}{n}\right)\right) = 0,$$

und da $\mathrm{val}\left(\frac{\omega}{n}\right)$ eine der ν Funktionen v_n ist, so ergibt sich aus der eben bewiesenen Irreduktibilität, daß $F_n(v, \sigma)$ durch $F_n(\sigma, v)$ teilbar und folglich $= \pm F_n(\sigma, v)$ sein muß; da aber im Falle des unteren Zeichens die irreduktible Funktion $F_n(\sigma, v)$ den Faktor $(\sigma - v)$ enthalten würde, so muß, wenn $n > 1$ ist, das obere Zeichen gelten.

Da die sämtlichen Funktionen v_n nur spezielle Fälle der in der Gleichung (11) des § 5 mit v' bezeichneten Funktion bilden, so besitzt die dortige Differentialgleichung (12) unendlich viele partikuläre Lösungen $v' = v_n$, welche algebraische Funktionen von v sind. Es

läßt sich auch zeigen, daß sie keine anderen algebraischen Lösungen besitzen kann, und hieraus kann man, wie ich glaube, den Satz ableiten, daß alle Koeffizienten der Funktion $F_n(\sigma, v)$ rationale Zahlen sind. Ich bemerke schließlich, daß man durch die Untersuchung der ganzen Funktion $F_n(v, v)$ oder auch der Diskriminante der Funktion $F_n(\sigma, v)$ zur Theorie der singulären Moduln geführt wird, für welche die komplexe Multiplikation der elliptischen Funktionen stattfindet; eine nähere Ausführung dieser Untersuchung, in welcher die Komposition der quadratischen Formen eine wesentliche Rolle spielt, muß ich mir aber für eine andere Gelegenheit versparen.

Braunschweig, den 12. Juni 1877.

Erläuterungen zur vorstehenden Abhandlung.

Es war zur Zeit der Entstehung dieser Abhandlung noch unbekannt, daß die hier von Dedekind beschriebene, später in der Theorie der Modulfunktionen so wichtig gewordene Dreiecksteilung der ω-Halbebene bereits weit früher aufgefunden worden war. Schon Gauß hat das Dreiecksnetz gekannt und benutzt, worüber man Bd. 8 seiner Werke, S. 102—105 vergleiche. Dasselbe gilt von Riemann, der in einer Vorlesung über die hypergeometrische Reihe im Wintersemester 1858/59 das Dreiecksnetz behandelt und zur Beschreibung der Abhängigkeit des Legendre-Jacobischen Integralmoduls k^2 vom Periodenverhältnis ω benutzt. Die Vorlesung ist s. Zt. durch v. Bezold nachgeschrieben; diese Nachschrift ist erst 1897 bekannt geworden und in den von M. Noether und W. Wirtinger herausgegebenen „Nachträgen zu Bernhard Riemanns gesammelten mathematischen Werken“ (Leipzig, 1902) allgemein zugänglich gemacht. Noch ehe die Abhandlung Dedekinds erschien, war F. Klein an die Theorie der elliptischen Modulfunktionen herangeführt. Seine erste ausführlichere Abhandlung über Modulfunktionen „Über die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünften Grades“ (datiert Anfang Mai 1878) ist mit Dedekinds Arbeit eng verwandt. Klein hat sich über die Entstehung seiner Arbeiten über Modulfunktionen selbst ausführlich ausgesprochen in Band 3 seiner „Gesammelten mathematischen Abhandlungen“, S. 3—9.

Fricke.

XV.

Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen.

[Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Bd. 23, S. 1—23 (1878).]

Die neuen Prinzipien, durch welche ich zu einer ausnahmelosen und strengen Theorie der Ideale gelangt bin, habe ich zuerst vor sieben Jahren in der zweiten Auflage der Vorlesungen über Zahlentheorie von Dirichlet (§§ 159—170) entwickelt und neuerdings in dem Bulletin des sciences mathématiques et astronomiques (t. XI, p. 278; t. I (2e série), p. 17, 69, 144, 207) ausführlicher und in etwas veränderter Form dargestellt. Mit demselben Gegenstand hatte ich mich schon vorher, durch die große Entdeckung Kummers angeregt, eine lange Reihe von Jahren hindurch beschäftigt, wobei ich von einer ganz anderen Grundlage, nämlich von der Theorie der höheren Kongruenzen ausging; allein obgleich diese Untersuchungen mich dem erstrebten Ziele sehr nahe brachten, so konnte ich mich zu ihrer Veröffentlichung doch nicht entschließen, weil die so entstandene Theorie hauptsächlich an zwei Unvollkommenheiten leidet. Die eine besteht darin, daß die Untersuchung eines Gebietes von ganzen algebraischen Zahlen sich zunächst auf die Betrachtung einer bestimmten Zahl und der ihr entsprechenden Gleichung gründet, welche als Kongruenz aufgefaßt wird, und daß die so erhaltenen Definitionen der idealen Zahlen (oder vielmehr der Teilbarkeit durch die idealen Zahlen) zufolge dieser bestimmt gewählten Darstellungsform nicht von vornherein den Charakter der Invarianz erkennen lassen, welcher in Wahrheit diesen Begriffen zukommt; die zweite Unvollkommenheit dieser Begründungsart besteht darin, daß bisweilen eigentümliche Ausnahmefälle auftreten, welche eine besondere Behandlung verlangen. Meine neuere Theorie dagegen gründet sich ausschließlich auf solche Begriffe, wie die des Körpers,

der ganzen Zahl, des Ideals, zu deren Definition es gar keiner bestimmten Darstellungsform der Zahlen bedarf, und wie hierdurch der erstgenannte Mangel von selbst wegfällt, so bewährt sich die Kraft dieser äußerst einfachen Begriffe auch darin, daß bei dem Beweise der allgemeinen Gesetze der Teilbarkeit eine Unterscheidung mehrerer Fälle gar niemals mehr auftritt. Über den Zusammenhang zwischen beiden Begründungsarten habe ich in den Göttingischen gelehrten Anzeigen vom 20. September 1871 (S. 1488—1492) einige Bemerkungen und Sätze ohne Beweis mitgeteilt, und namentlich habe ich daselbst den Grund aufgedeckt, auf welchem das Auftreten der erwähnten eigentümlichen Ausnahmefälle beruht. Seitdem ist im Jahre 1874 eine Theorie der idealen Zahlen von Zolotareff erschienen, welche in russischer Sprache abgefaßt und unter dem Titel Théorie des nombres entiers complexes, avec une application au calcul intégral im Jahrbuch über die Fortschritte der Mathematik (Bd. 6, S. 117) angezeigt und kurz besprochen ist. Aus dieser Anzeige*) geht hervor, daß die Theorie von Zolotareff sich ebenfalls auf die Theorie der höheren Kongruenzen gründet, daß aber gerade die Behandlung der erwähnten Ausnahmefälle vorläufig ausgeschlossen und einer späteren Darstellung vorbehalten ist. Ich weiß nicht, ob diese in Aussicht gestellte Vervollständigung seitdem veröffentlicht worden ist; da aber der Zusammenhang zwischen den beiden Begründungsarten der allgemeinen Idealtheorie an sich ein hinreichendes Interesse besitzt, so erlaube ich mir, im folgenden die Beweise zu den in den Göttingischen gelehrten Anzeigen mitgeteilten Bemerkungen nachzuliefern. Hierbei muß ich sowohl meine Theorie der Ideale, als auch die Theorie der höheren Kongruenzen, von welcher ich früher in Borchardts Journal (Bd. 54, S. 1) eine gedrängte Darstellung gegeben habe, als bekannt voraussetzen; der Kürze halber werde ich diese Abhandlung über die Kongruenzen mit C., die zweite Auflage der Zahlentheorie von Dirichlet mit D., und die oben angeführte Abhandlung im Bulletin des sciences mathématiques mit B. zitieren.

*) Nur auf diese kann ich mich hier berufen; zwar habe ich das Originalwerk nach mehreren vergeblichen Versuchen, es mir im Buchhandel zu verschaffen, kürzlich durch die Güte des Herrn Prof. Wangerin geliehen erhalten, aber bei meiner Unkenntnis der russischen Sprache habe ich zu meinem großen Bedauern nur das Wenige verfolgen können, was schon aus dem Anblick der Formeln verständlich ist.

§ 1.

Es sei Ω ein endlicher Körper vom Grade n, und $\mathfrak{o}$ das Gebiet aller in Ω enthaltenen ganzen Zahlen, so gibt es immer eine aus n voneinander unabhängigen ganzen Zahlen

$$\omega_1,\ \omega_2 \cdots \omega_n$$

bestehende Basis des Gebietes $\mathfrak{o}$, d. h. das System $\mathfrak{o}$ ist identisch mit dem Inbegriffe

$$[\omega_1,\ \omega_2 \cdots \omega_n]$$

aller Zahlen ω von der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

wo

$$h_1,\ h_2 \cdots h_n$$

willkürliche ganze rationale Zahlen bedeuten; die Diskriminante

$$\Delta(\omega_1,\ \omega_2 \cdots \omega_n) = \Delta(\Omega) = D,$$

welche von der Wahl der Basiszahlen $\omega_1, \omega_2 \cdots \omega_n$ unabhängig ist, heißt die Grundzahl oder die Diskriminante des Körpers Ω (D. §§ 159, 160, 162; B. §§ 13—18).

Ist nun θ eine bestimmte ganze Zahl des Körpers, so kann man

$$\begin{aligned}
1 &= c_1^0\omega_1 + c_2^0\omega_2 + \cdots + c_n^0\omega_n\\
\theta &= c_1'\omega_1 + c_2'\omega_2 + \cdots + c_n'\omega_n\\
\theta^2 &= c_1''\omega_1 + c_2''\omega_2 + \cdots + c_n''\omega_n\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\theta^{n-1} &= c_1^{(n-1)}\omega_1 + c_2^{(n-1)}\omega_2 + \cdots + c_n^{(n-1)}\omega_n
\end{aligned}$$

setzen, wo die sämtlichen n^2 Koeffizienten oder Koordinaten c ganze rationale Zahlen bedeuten, und es ist

$$\Delta(1,\ \theta,\ \theta^2 \cdots \theta^{n-1}) = Dk^2,$$

wo

$$k = \sum \pm c_1^0 c_2' \cdots c_n^{(n-1)}$$

eine ganze rationale Zahl ist; diese Zahl k, deren absoluter Wert von der Wahl der Basiszahlen $\omega_1, \omega_2 \cdots \omega_n$ unabhängig ist, soll im folgenden der Kürze halber der Index der ganzen Zahl θ genannt werden. Ist k, wie wir immer voraussetzen werden, von 0 verschieden, so sind die n Zahlen

$$1,\ \theta,\ \theta^2 \cdots \theta^{n-1}$$

voneinander unabhängig (D. § 159; B. §§ 4, 15, 17) und θ ist die Wurzel einer irreduktiblen Gleichung n^{ten} Grades

$$F(\theta) = \theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_n = 0,$$

deren Koeffizienten $1, a_1, a_2 \cdots a_n$ ganze rationale Zahlen sind.

Bedeutet ferner $\varphi(t)$ jede beliebige Funktion der Variabelen t, — und ich bemerke ein für allemal, daß unter diesem Namen und unter einem Zeichen von der Form $\varphi(t)$, $f(t)\cdots$ in der gegenwärtigen Abhandlung ausschließlich eine ganze Funktion von t verstanden werden soll, deren Koeffizienten ganze rationale Zahlen sind —, so bildet der Inbegriff $\mathfrak{o}'$ aller Zahlen von der Form

$$\omega' = \varphi(\theta)$$

eine sogenannte Ordnung (D. §§ 165, 166; B. § 23); alle diese Zahlen sind ganze Zahlen des Körpers Ω und folglich auch in $\mathfrak{o}$ enthalten. Offenbar ist es gestattet, nur solche Funktionen

$$\varphi(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_{n-1} t^{n-1}$$

zu betrachten, deren Grad kleiner als n ist; denn wenn der Grad einer Funktion $\varphi_1(t)$ gleich n oder größer ist, so liefert sie, durch die Funktion

$$F(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n$$

dividiert, einen Rest $\varphi(t)$ von niedrigerem Grade als n, und gleichzeitig ist $\varphi_1(\theta) = \varphi(\theta)$; mit Benutzung einer schon oben gebrauchten Bezeichnungsweise (B. § 3) kann man daher

$$\mathfrak{o}' = [1, \theta, \theta^2 \cdots \theta^{n-1}]$$

setzen. Außerdem ergibt sich aus der Irreduktibilität der Gleichung $F(\theta) = 0$, daß jede Zahl ω' nur auf eine einzige Weise in dieser letzteren Form $\varphi(\theta)$ darstellbar ist; doch werden wir uns im folgenden durchaus nicht immer auf diese Darstellungsform der Zahlen ω' beschränken, vielmehr auch Funktionen von beliebig hohem Grade zulassen.

Die sämtlichen Primzahlen p — mit welchem Namen stets rationale, positive Primzahlen bezeichnet sein sollen — zerfallen nun, nachdem einmal eine bestimmte Zahl θ gewählt und der Darstellung zugrunde gelegt ist, in zwei verschiedene Arten; die erste Art besteht aus den unendlich vielen Primzahlen, welche in dem Index k der Zahl θ nicht aufgehen; falls $k = \pm 1$ ist, gehören alle Primzahlen dieser ersten Art an, und $\mathfrak{o}'$ ist identisch mit $\mathfrak{o}$. Wenn aber $k^2 > 1$ ist, so gibt es eine endliche Anzahl von Primzahlen der zweiten Art, nämlich solchen, welche in k aufgehen. Es wird sich im folgenden Paragraphen zeigen, daß die Zerlegung der Primzahlen p der ersten Art, oder vielmehr die Zerlegung der ihnen entsprechenden

Hauptideale $\mathfrak{o}\,p$*) in Produkte aus lauter Primidealen sich vollständig zurückführen läßt auf die Zerlegung der Funktion $F(t)$ in ein Produkt aus lauter Primfunktionen in bezug auf den Modul p (C. 6), während dies für Primzahlen der zweiten Art nicht in gleich einfacher Weise möglich ist. Dieser Untersuchung sind folgende Bemerkungen vorauszuschicken.

Es sei p eine bestimmte Primzahl der ersten Art, also k nicht teilbar durch p. In diesem Falle ist eine in $\mathfrak{o}'$ enthaltene Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

nur dann durch p teilbar (also von der Form $p\,\omega$, wo ω eine ganze, d. h. in $\mathfrak{o}$ enthaltene Zahl bedeutet), wenn alle Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ durch p teilbar sind; denn setzt man

$$\begin{aligned}
h_1 &= c_1^0 x_0 + c_1' x_1 + c_1'' x_2 + \cdots + c_1^{(n-1)} x_{n-1}\\
h_2 &= c_2^0 x_0 + c_2' x_1 + c_2'' x_2 + \cdots + c_2^{(n-1)} x_{n-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
h_n &= c_n^0 x_0 + c_n' x_1 + c_n'' x_2 + \cdots + c_n^{(n-1)} x_{n-1},
\end{aligned}$$

so ist

$$\omega' = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

und wenn ω' durch p teilbar sein soll, so muß (zufolge der Bedeutung von ω_1, $\omega_2 \cdots \omega_n$) jede der Koordinaten h_1, $h_2 \cdots h_n$ durch p teilbar sein; hieraus ergibt sich aber weiter, daß die Produkte $k\,x_0$, $k\,x_1$, $k\,x_2 \cdots k\,x_{n-1}$, und folglich auch die Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ sämtlich durch p teilbar sein müssen, wie behauptet war. Denselben Satz kann man offenbar auch so aussprechen: ist eine Zahl ω' der Ordnung $\mathfrak{o}'$ teilbar durch eine Primzahl p der ersten Art, so ist auch der Quotient ω'/p eine Zahl derselben Ordnung $\mathfrak{o}'$. Umgekehrt, wenn alle Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ durch p teilbar sind, so ist selbstverständlich auch ω' durch p teilbar. Es sind daher zwei Zahlen $\varphi_1(\theta)$ und $\varphi_2(\theta)$ der Ordnung $\mathfrak{o}'$ stets und nur dann einander kongruent nach dem Modul p, d. h. ihre Differenz $\varphi_1(\theta) - \varphi_2(\theta)$ ist teilbar durch p, wenn je zwei entsprechende Koeffizienten der beiden Funktionen $\varphi_1(t)$ und $\varphi_2(t)$ einander nach p kongruent sind, d. h. in der Bezeichnungsweise der Theorie der höheren Kongruenzen, wenn

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p}$$

*) Diese Bezeichnung der Hauptideale ist zweckmäßiger als diejenige $\mathfrak{i}(p)$, welche ich früher (D. § 163) gebraucht habe.

ist (C. 1). Hierbei war aber vorausgesetzt, daß die Grade der Funktionen $\varphi_1(t)$, $\varphi_2(t)$ kleiner als n waren; ist dies nicht der Fall, so erhält man durch Division mit $F(t)$ eine Identität von der Form

$$\varphi_1(t) - \varphi_2(t) = F(t)\psi(t) + \psi_1(t),$$

wo $\psi_1(t)$ von niedrigerem Grade als n ist, und hieraus $\varphi_1(\theta) - \varphi_2(\theta) = \psi_1(\theta)$; soll nun

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

sein, so muß nach dem obigen $\psi_1(t) = p\,\psi_2(t)$, also

$$\varphi_1(t) - \varphi_2(t) = F(t)\psi(t) + p\,\psi_2(t)$$

sein; das Stattfinden einer solchen Identität bezeichnet man aber in der Theorie der höheren Kongruenzen durch

$$\varphi_1(t) - \varphi_2(t) \equiv F(t)\psi(t) \pmod{p}$$

oder noch kürzer (C. 7) durch

$$\varphi_1(t) \equiv \varphi_2(t) \quad (\text{modd. } p,\ F(t)).$$

Umgekehrt leuchtet ein, daß aus dieser letzten Funktionenkongruenz auch wieder die Zahlenkongruenz

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

folgt; beide Kongruenzen sind daher gleichbedeutend. Mithin gibt es in $\mathfrak{o}'$ genau ebenso viele nach p inkongruente Zahlen $\varphi(\theta)$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppelmodul p, $F(t)$ gibt; da nun die Anzahl der letzteren $= p^n$ ist (C. 8), und da die Anzahl $(\mathfrak{o}, \mathfrak{o}\,p) = N(p)$ aller in $\mathfrak{o}$ enthaltenen, nach p inkongruenten Zahlen genau ebenso groß ist (B. § 18; D. § 162), so ergibt sich das wichtige Resultat: **jede Zahl ω des Gebietes $\mathfrak{o}$ ist mit einer Zahl $\omega' = \varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul p.**

Zu derselben Folgerung gelangt man unmittelbar auch durch folgende einfache Betrachtung. Aus den n Relationen zwischen den Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ einerseits und den Zahlen $\omega_1, \omega_2 \cdots \omega_n$ andererseits geht hervor, daß die Produkte $k\omega_1, k\omega_2 \cdots k\omega_n$ und folglich auch alle Produkte von der Form $k\omega$, wo ω jede beliebige Zahl in $\mathfrak{o}$ bedeutet, in der Ordnung $\mathfrak{o}'$ enthalten sind; man kann daher $k\omega = \varphi(\theta)$ setzen. Da nun k durch die Primzahl p nicht teilbar ist, so kann man die ganze rationale Zahl l so wählen, daß $kl \equiv 1 \pmod{p}$ wird, und hieraus folgt $\omega \equiv lk\omega \equiv l\varphi(\theta) \pmod{p}$; also ist ω wirklich mit einer Zahl $l\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul p.

Ganz anders verhält es sich dagegen, wenn p eine Primzahl der zweiten Art ist; da in diesem Falle die Determinante k durch p teilbar ist, so kann man nach einem Satze, dessen sehr leichten Beweis ich hier wohl übergehen darf, n ganze rationale Zahlen x_0, $x_1 \cdots x_{n-1}$, die nicht alle durch p teilbar sind, so wählen, daß die oben mit h_1, $h_2 \cdots h_n$ bezeichneten Summen sämtlich durch p teilbar werden; dann ist die entsprechende Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

der Ordnung $\mathfrak{o}'$ wirklich teilbar durch p, obgleich ihre Koeffizienten x_0, $x_1 \cdots x_{n-1}$ nicht alle durch p teilbar sind. Hieraus folgt sofort, daß die Anzahl $(\mathfrak{o}', \mathfrak{o}\,p)$ der in $\mathfrak{o}'$ enthaltenen, nach p inkongruenten Zahlen kleiner als p^n ist, und folglich gibt es in $\mathfrak{o}$ Zahlen ω, welche mit keiner in $\mathfrak{o}'$ enthaltenen Zahl $\varphi(\theta)$ nach p kongruent sind, d. h. es gibt Zahlklassen (mod. p) in $\mathfrak{o}$, für welche in $\mathfrak{o}'$ kein Repräsentant vorhanden ist. Die genaue Bestimmung der Anzahl $(\mathfrak{o}', \mathfrak{o}\,p)$ ist für unseren Hauptzweck nicht erforderlich [*)].

§ 2.

In diesem Paragraphen machen wir durchweg die Voraussetzung, daß p eine Primzahl der ersten Art ist, und wir wollen beweisen, daß in diesem Falle die Theorie der höheren Kongruenzen ein einfaches Mittel gibt, um das Hauptideal $\mathfrak{o}\,p$ in seine Primfaktoren zu zerlegen. Dies geschieht dadurch, daß die Funktion $F(t)$, die wir kürzer auch durch F bezeichnen werden, nach dem Modul p als Produkt von lauter Primfunktionen $P(t)$ dargestellt wird (C. 6); der bequemeren Ausdrucksweise halber wollen wir, was erlaubt ist, jede Primfunktion P so wählen, daß ihr höchster Koeffizient $= 1$ ist, woraus folgt, daß zwei inkongruente Primfunktionen auch immer relative Primfunktionen sein werden (C. 5). Durch Vereinigung aller einander kongruenten Faktoren in eine Potenz erhält man

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo P_1, $P_2 \cdots P_m$ die sämtlichen inkongruenten, in F aufgehenden Primfunktionen bedeuten.

[*) Schon bei Zolotareff (Mélanges math. et astron. du Bulletin de l'academie, St. Petersburg, Bd. 5, 13./25. September 1877) findet man den Satz, daß die Ausnahmeprimzahlen eben diejenigen sind, wofür eine durch p teilbare Zahl ω' in der Ordnung $\mathfrak{o}'$ vorkommt, worin nicht alle Koeffizienten durch p teilbar sind. Zolotareff zeigt aber nicht, daß diese Primzahlen eben die Indexteiler sind.]

Ist nun P eine beliebige dieser m Primfunktionen, und $\varrho = P(\theta)$, so entspricht derselben ein bestimmtes Ideal $\mathfrak{p}$, welches wir als den größten gemeinschaftlichen Teiler der beiden Hauptideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ definieren. Um die Eigenschaften dieses Ideals $\mathfrak{p}$ festzustellen, betrachten wir zunächst alle diejenigen in der Ordnung $\mathfrak{o}'$ enthaltenen Zahlen $\psi(\theta)$, welche durch $\mathfrak{p}$ teilbar (d. h. in $\mathfrak{p}$ enthalten) sind, und wir wollen beweisen, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}} \tag{1}$$

völlig gleichbedeutend ist mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p, P}. \tag{2}$$

In der Tat, da das Ideal $\mathfrak{p}$ zufolge seiner Definition (D. § 163; B. § 19) der Inbegriff aller Zahlen von der Form

$$\varrho\,\alpha + p\,\beta$$

ist, wo α, β willkürliche Zahlen des Gebiets $\mathfrak{o}$ bedeuten, und da (nach § 1) jede Zahl α mit einer Zahl $\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent ist nach dem Modul p, so folgt aus (1) eine Kongruenz von der Form

$$\psi(\theta) \equiv P(\theta)\,\varphi(\theta) \pmod{p};$$

hieraus ergibt sich aber (nach § 1) die Funktionenkongruenz

$$\psi(t) \equiv P(t)\,\varphi(t) \pmod{p, F},$$

also auch die Kongruenz (2), weil F durch P teilbar ist. Umgekehrt folgt aus (2) unmittelbar, daß $\psi(\theta)$ von der Form $\varrho\,\alpha + p\,\beta$, also $\equiv 0 \pmod{\mathfrak{p}}$ sein muß, womit die obige Behauptung bewiesen ist.

Mit Hilfe dieses Resultats kann man leicht die Norm des Ideals $\mathfrak{p}$, d. h. die Anzahl $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{p}$ inkongruenten Zahlen bestimmen. Sind nämlich α_1, α_2 zwei beliebige Zahlen in $\mathfrak{o}$, so gibt es (nach § 1) in $\mathfrak{o}'$ zwei Zahlen $\varphi_1(\theta)$, $\varphi_2(\theta)$, welche resp. den Zahlen α_1, α_2 nach p kongruent sind, und da p durch $\mathfrak{p}$ teilbar ist, so ist auch

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}};$$

die beiden Zahlen α_1, α_2 sind daher stets und nur dann kongruent in bezug auf $\mathfrak{p}$, wenn

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{\mathfrak{p}}$$

ist; diese Kongruenz ist aber nach dem obigen gleichbedeutend mit der Kongruenz

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p, P};$$

es gibt daher in $\mathfrak{o}$ genau ebenso viele inkongruente Zahlen α in bezug auf $\mathfrak{p}$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppel-

modul p, P gibt, und da die Anzahl der letzteren $= p^f$ ist, wo f den Grad der Funktion P bedeutet (C. 8), so erhalten wir

$$N(\mathfrak{p}) = p^f.$$

Ebenso leicht ergibt sich, daß $\mathfrak{p}$ ein Primideal ist. Da nämlich $f \geqq 1$, also $N(\mathfrak{p}) > 1$ ist, so ist $\mathfrak{p}$ jedenfalls von 0 verschieden, und es braucht daher nur noch gezeigt zu werden, daß $\mathfrak{p}$ kein zusammengesetztes Ideal, d. h. kein Produkt von der Form $\mathfrak{a}_1 \mathfrak{a}_2$ ist, wo die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von 0 verschieden sind (D. § 163; B. § 25, 4°). Ein solches zusammengesetztes Ideal $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ besitzt die charakteristische Eigenschaft, daß immer zwei durch $\mathfrak{m}$ nicht teilbare Zahlen α_1, α_2 existieren, deren Produkt $\alpha_1 \alpha_2$ durch $\mathfrak{m}$ teilbar ist; denn weil die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von 0 verschieden sind, so kann auch keines von ihnen durch ihr Produkt $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ teilbar sein, und folglich gibt es eine durch $\mathfrak{a}_1$, aber nicht durch $\mathfrak{m}$ teilbare Zahl α_1, und ebenso eine durch $\mathfrak{a}_2$, aber nicht durch $\mathfrak{m}$ teilbare Zahl α_2, und offenbar ist $\alpha_1 \alpha_2$ teilbar durch $\mathfrak{m}$. Es wird daher $\mathfrak{p}$ gewiß ein Primideal sein, wenn wir beweisen können, daß ein Produkt $\alpha_1 \alpha_2$ nur dann durch $\mathfrak{p}$ teilbar ist, wenn wenigstens einer der Faktoren α_1, α_2 durch $\mathfrak{p}$ teilbar ist. Zu diesem Zweck setzen wir, wie oben,

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}},$$

so ist

$$\alpha_1 \alpha_2 \equiv \varphi_1(\theta)\, \varphi_2(\theta) \pmod{\mathfrak{p}};$$

soll nun $\alpha_1 \alpha_2 \equiv 0 \pmod{\mathfrak{p}}$ sein, so muß auch

$$\varphi_1(\theta)\, \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

mithin

$$\varphi_1(t)\, \varphi_2(t) \equiv 0 \pmod{p, P}$$

sein; da aber P eine Primfunktion ist, so muß wenigstens eine der beiden Kongruenzen

$$\varphi_1(t) \equiv 0, \quad \varphi_2(t) \equiv 0 \pmod{p, P}$$

stattfinden (C. 6), also auch wenigstens eine der Kongruenzen

$$\varphi_1(\theta) \equiv 0, \quad \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

d. h. wenigstens eine der beiden Zahlen α_1, α_2 muß $\equiv 0 \pmod{\mathfrak{p}}$ sein. Also ist $\mathfrak{p}$ ein Primideal; und zwar sagen wir (B. § 21), daß $\mathfrak{p}$ ein Primideal vom Grade f ist, weil $N(\mathfrak{p}) = p^f$ ist.

Jetzt wollen wir beweisen, daß der Exponent e der höchsten in F aufgehenden Potenz von P zugleich der Exponent der höchsten in p aufgehenden Potenz des Primideals $\mathfrak{p}$ ist. In der Tat, wenn F nach dem Modul p durch P^e, aber nicht durch P^{e+1} teilbar ist, so kann man

$$F \equiv S P^e \pmod{p}$$

setzen, wo S nicht teilbar durch P ist, woraus nach dem Obigen folgt, daß die Zahl

$$\sigma = S(\theta)$$

nicht durch $\mathfrak{p}$ teilbar ist. Da ferner $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ ist, so können wir

$$\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{a}, \quad \mathfrak{o}\,\varrho = \mathfrak{p}\,\mathfrak{b}$$

setzen, wo $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten, und wir haben zu beweisen, daß $\mathfrak{p}^{e-1}$ die höchste in $\mathfrak{a}$ aufgehende Potenz von $\mathfrak{p}$ ist. Zu diesem Zwecke betrachten wir die Zahl

$$\eta = \sigma\,\varrho^{e-1} = S(\theta)\,P(\theta)^{e-1};$$

dieselbe kann nicht durch p teilbar sein, weil der Grad der Funktion $S\,P^{e-1}$ kleiner als n, und weil ihr höchster Koeffizient $= 1$ ist; aber η ist teilbar durch $\mathfrak{p}^{e-1}$, weil ϱ durch $\mathfrak{p}$ teilbar ist. Vermöge der Kongruenz $F \equiv S\,P^e \pmod{p}$ ist nun das Produkt $\eta\,\varrho = \sigma\,\varrho^e$ teilbar durch p, also ist auch das Ideal $\eta\,\mathfrak{p}\,\mathfrak{b}$ teilbar durch $\mathfrak{p}\,\mathfrak{a}$, mithin $\eta\,\mathfrak{b}$ teilbar durch $\mathfrak{a}$, folglich η teilbar durch $\mathfrak{a}$, weil $\mathfrak{a}$ und $\mathfrak{b}$ relative Primideale sind. Man kann daher

$$\mathfrak{o}\,\eta = \mathfrak{a}\,\mathfrak{c}$$

setzen, wo $\mathfrak{c}$ ein Ideal bedeutet, welches nicht durch $\mathfrak{p}$ teilbar ist*), weil sonst η durch $\mathfrak{a}\,\mathfrak{p}$, also durch p teilbar wäre, was nicht der Fall ist. Da nun η durch $\mathfrak{p}^{e-1}$ teilbar ist, so muß auch $\mathfrak{a}$ durch $\mathfrak{p}^{e-1}$ teilbar sein. Wir haben jetzt nur noch zu zeigen, daß $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar ist. Da $e \geqq 1$ ist, so müßte, wenn $\mathfrak{a}$ durch $\mathfrak{p}^e$ teilbar wäre, jedenfalls $\mathfrak{a}$ durch $\mathfrak{p}$ selbst teilbar sein; sobald aber $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar ist, kann $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich ist dann ϱ nicht teilbar durch $\mathfrak{p}^2$; da ferner σ nicht durch $\mathfrak{p}$ teilbar ist, so ist in diesem Falle $\mathfrak{p}^{e-1}$ die höchste in der Zahl $\eta = \sigma\,\varrho^{e-1}$ aufgehende Potenz von $\mathfrak{p}$, und folglich kann das in η aufgehende Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar sein, w. z. b. w.

Nachdem die Untersuchung für eine bestimmte in F aufgehende Primfunktion P und für das ihr entsprechende Primideal $\mathfrak{p}$ so weit geführt ist, wenden wir dieselbe auf alle in der Funktion

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

*) Es ist daher $\mathfrak{a}$ der größte gemeinschaftliche Teiler, und folglich $\eta\,\mathfrak{p}$ das kleinste gemeinschaftliche Vielfache der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\eta$, d. h. $\mathfrak{p}$ ist der Inbegriff aller Wurzeln π der Kongruenz $\eta\,\pi \equiv 0 \pmod{p}$. Dies hätte auch als Definition des Ideals $\mathfrak{p}$ benutzt werden können.

aufgehenden, inkongruenten Primfunktionen

$$P_1,\ P_2 \cdots P_m$$

an, deren Grade wir resp. mit

$$f_1,\ f_2 \cdots f_m$$

bezeichnen; die diesen Funktionen entsprechenden Primideale

$$\mathfrak{p}_1,\ \mathfrak{p}_2 \cdots \mathfrak{p}_m$$

haben resp. dieselben Grade, d. h. es ist

$$N(\mathfrak{p}_1) = p^{f_1},\quad N(\mathfrak{p}_2) = p^{f_2} \cdots N(\mathfrak{p}_m) = p^{f_m},$$

und

$$\mathfrak{p}^{e_1},\ \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

sind die höchsten in p aufgehenden Potenzen dieser Ideale. Diese m Primideale sind verschieden voneinander; denn da z. B. P_2 nicht durch P_1 teilbar ist (mod. p), so ist die durch $\mathfrak{p}_2$ teilbare Zahl $P_2(\theta)$ nicht durch $\mathfrak{p}_1$ teilbar, und folglich sind $\mathfrak{p}_1$, $\mathfrak{p}_2$ verschiedene Primideale. Endlich bemerken wir, daß p durch kein anderes Primideal teilbar sein kann; da nämlich

$$P_1(\theta)^{e_1} P_2(\theta)^{e_2} \cdots P_m(\theta)^{e_m} \equiv 0 \pmod{p}$$

ist, so muß ein in p aufgehendes Primideal auch in einer der m Zahlen $\varrho = P(\theta)$ aufgehen und folglich mit dem Primideal $\mathfrak{p}$ identisch sein, welches der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ ist.

Aus allen diesem folgt (D. § 163; B. § 25), daß

$$\mathfrak{o}p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

ist, und eine Bestätigung dieses Resultats ergibt sich durch die Betrachtung der Normen, wenn man berücksichtigt, daß

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

ist. Es ist somit folgender Satz bewiesen, den ich zuerst in den Göttingischen gelehrten Anzeigen vom 20. September 1871 ohne Beweis mitgeteilt habe:

I. Ist der Index k der Zahl θ, welche der irreduktiblen Gleichung n^{ten} Grades $F(\theta) = 0$ genügt, nicht teilbar durch die Primzahl p, und ist

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo P_1, $P_2 \cdots P_m$ inkongruente Primfunktionen resp. vom Grade f_1, $f_2 \cdots f_m$ bedeuten, so ist

$$\mathfrak{o}p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschiedene Primideale resp. vom Grade $f_1, f_2 \cdots f_m$ sind, und zwar entspricht je einer Primfunktion P ein bestimmtes Primideal $\mathfrak{p}$ in der Weise, daß $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}p$ und $\mathfrak{o}P(\theta)$ ist.

§ 3.

Aus diesem Satze geht hervor, daß man bei Zugrundelegung einer bestimmten ganzen Zahl θ des Körpers Ω, welche zur Darstellung von unendlich vielen ganzen Zahlen $\varphi(\theta)$ dient, mit voller Sicherheit die Zerlegung aller derjenigen Primzahlen p findet, welche nicht in dem Index k dieser Zahl θ aufgehen; es ist daher von großer Wichtigkeit zu wissen, ob eine Primzahl p in dem Index k aufgeht oder nicht. Sobald freilich eine Basis $\omega_1, \omega_2 \cdots \omega_n$ des Gebiets $\mathfrak{o}$, oder auch nur die Grundzahl D des Körpers Ω bekannt ist, erledigt sich diese Frage sehr leicht, weil hieraus k direkt gefunden werden kann; denn aus den Koeffizienten der Gleichung $F(\theta) = 0$ läßt sich ihre Diskriminante

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(F'(\theta)) = Dk^2,$$

und hieraus durch Division mit D das Quadrat des Index k bestimmen. Bei den meisten Untersuchungen liegt aber die Sache ganz anders, nämlich so, daß nur die Gleichung $F(\theta) = 0$, nicht aber die Grundzahl D des ihr entsprechenden Körpers Ω gegeben ist; es kommt darauf an zu entscheiden, ob eine bestimmte Primzahl p in dem noch unbekannten Index k der Zahl θ aufgeht oder nicht. Dies gelingt nun in der Tat, wie wir jetzt zeigen wollen, mit Hilfe der Theorie der höheren Kongruenzen, und zwar hängt die Entscheidung, wenn wir die früheren Bezeichnungen beibehalten, wesentlich von der Beschaffenheit der Funktion M ab, welche in der Identität

$$F = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} - pM$$

auftritt. Dies ergibt sich aus den beiden folgenden Sätzen.

II. Ist der Index k der Zahl θ nicht teilbar durch p, so kann M nach dem Modul p durch keine Primfunktion P teilbar sein, deren Quadrat in F aufgeht.

Zum Beweise dürfen wir alle Folgerungen benutzen, welche im vorigen Paragraphen aus der Annahme gezogen sind, daß k nicht

durch p teilbar ist. Indem wir alle dort gebrauchten Bezeichnungen beibehalten, setzen wir $F \equiv S P^e \pmod{p}$, also

$$F = S P^e - p M,$$

und nehmen an, es sei $e \geqq 2$; dann ist p teilbar durch $\mathfrak{p}^2$, folglich $\mathfrak{a}$ teilbar durch $\mathfrak{p}$, mithin $\mathfrak{b}$ nicht teilbar durch $\mathfrak{p}$. Es ist daher $\mathfrak{p}^e$ die höchste in der Zahl

$$S(\theta)\, P(\theta)^e = p M(\theta)$$

aufgehende Potenz von $\mathfrak{p}$, und da p durch $\mathfrak{p}^e$ teilbar ist, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich kann die Funktion M auch nicht $\equiv 0$ (modd. p, P) sein, w. z. b. w.

Auch ohne Benutzung der im vorigen Paragraphen gewonnenen Resultate läßt sich derselbe Satz leicht in der folgenden indirekten, aber vollständig äquivalenten Form beweisen:

Ist F nach dem Modul p teilbar durch das Quadrat einer Primfunktion P, also

$$F = S P^e - p M,$$

wo $e \geqq 2$, und ist M teilbar durch P, so muß der Index k der Zahl θ durch die Primzahl p teilbar sein.

Behalten die Buchstaben ϱ, σ, η dieselbe Bedeutung, wie im vorigen Paragraphen, setzen wir also

$$\varrho = P(\theta), \quad \sigma = S(\theta), \quad \eta = \sigma \varrho^{e-1},$$

so wird (nach § 1) der Beweis unseres Satzes geführt sein, wenn wir zeigen, daß unter den jetzigen Annahmen die Zahl $\eta = S(\theta)\, P(\theta)^{e-1}$ durch p teilbar sein muß; denn die Funktion $S P^{e-1}$ ist von niedrigerem Grade als n und auch nicht $\equiv 0 \pmod{p}$. Die Zahl η wird ferner gewiß durch p teilbar sein, wenn bewiesen wird, daß alle in p aufgehenden Potenzen von Primidealen auch in η aufgehen (D. § 163, B. § 25). Zu diesem Zweck setzen wir

$$\mu = M(\theta)$$

und betrachten die Gleichung

$$\sigma \varrho^e = \eta \varrho = p \mu.$$

Ist nun $\mathfrak{p}$ ein in p, aber nicht in ϱ aufgehendes Primideal, so folgt aus $\eta \varrho = p \mu$ unmittelbar, daß η durch die höchste in p aufgehende Potenz von $\mathfrak{p}$ teilbar ist. Ist aber $\mathfrak{p}$ ein in p und gleichzeitig in ϱ aufgehendes Primideal, so ergibt sich folgendes. Da S und P relative

Primfunktionen sind, so existieren zwei Funktionen U, V, welche der Kongruenz

$$S\,U + P\,V \equiv 1 \pmod{p}$$

genügen (C. 4); hieraus ergeben sich die Zahlenkongruenzen

$$\sigma\,U(\theta) + \varrho\,V(\theta) \equiv 1 \pmod{p}$$
$$\sigma\,U(\theta) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist σ nicht teilbar durch $\mathfrak{p}$. Sind daher $\mathfrak{p}^h$, $\mathfrak{p}^r$, $\mathfrak{p}^m$ die höchsten resp. in p, ϱ, μ aufgehenden Potenzen von $\mathfrak{p}$, so folgt aus $\sigma\varrho^e = p\mu$ und $\eta = \sigma\varrho^{e-1}$, daß

$$er = h + m,$$

und daß der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$ gleich

$$(e-1)r = h + m - r$$

ist; um daher wieder zu beweisen, daß η durch $\mathfrak{p}^h$ teilbar ist, brauchen wir nur noch zu zeigen, daß

$$m \geqq r$$

ist. Hierbei unterscheiden wir zwei Fälle. Ist erstens $r \geqq h$, so verwerten wir die erste Annahme unseres Satzes, derzufolge $e \geqq 2$ ist; hieraus folgt in der Tat $h + m = er \geqq 2r$, mithin $m - r \geqq r - h \geqq 0$, wie behauptet war. Ist aber zweitens $r \leqq h$, so benutzen wir die zweite Annahme unseres Satzes, derzufolge $M \equiv 0$ (modd. p, P), d. h. $M \equiv P\,T \pmod{p}$, also $\mu \equiv \varrho\,T(\theta) \pmod{p}$ ist; da nun sowohl ϱ, als auch p durch $\mathfrak{p}^r$ teilbar ist, so folgt aus dieser Kongruenz, daß auch μ durch $\mathfrak{p}^r$ teilbar, d. h. daß $m \geqq r$ ist, w. z. b. w.

Nachdem der Satz II auf zwei verschiedene Arten bewiesen ist, behaupten wir auch die Richtigkeit des umgekehrten Satzes:

III. **Ist M durch keine solche Primfunktion P teilbar (mod. p), deren Quadrat zugleich in F aufgeht, so ist der Index k der Zahl θ nicht teilbar durch p.**

Derselbe Satz kann offenbar auch in der folgenden Form ausgesprochen werden:

Ist der Index k der Zahl θ teilbar durch die Primzahl p, so gibt es eine in M aufgehende Primfunktion P, deren Quadrat zugleich in F aufgeht (mod. p).

Dem Beweise legen wir die letztere Form zugrunde, weil die Annahme, daß k durch p teilbar ist, eine leichtere Verwertung gestattet, insofern aus ihr (nach § 1) die Existenz einer durch p teilbaren Zahl

$$\varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

folgt, deren Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ nicht alle durch p teilbar sind. Bezeichnet man nun mit A den größten gemeinschaftlichen Teiler der beiden Funktionen $\varphi(t)$ und F nach dem Modul p, so ist der Grad von A kleiner als n, weil φ von niedrigerem Grade als n und auch nicht $\equiv 0 \pmod{p}$ ist; setzt man daher

$$F = AB - pM,$$

so ist B keine Konstante. Nun existieren zwei Funktionen φ_1, φ_2, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + F(t)\,\varphi_2(t) \equiv A(t) \pmod{p}$$

genügen (C. 4); hieraus ergibt sich, daß die Zahl $A(\theta)$ ebenfalls durch p teilbar ist*) und folglich einer Gleichung von der Form

$$A(\theta)^s + p h_1 A(\theta)^{s-1} + p^2 h_2 A(\theta)^{s-2} + \cdots + p^s h_s = 0$$

genügt, wo $h_1, h_2 \cdots h_s$ ganze rationale Zahlen bedeuten (D. § 160; B. § 13). Da die Gleichung $F(\theta) = 0$ irreduktibel ist, so ergibt sich hieraus eine in bezug auf die Variable t identische Gleichung von der Form

$$A^s + p h_1 A^{s-1} + p^2 h_2 A^{s-2} + \cdots + p^s h_s = F G,$$

also auch die Kongruenz

$$A^s \equiv 0 \pmod{p, F};$$

mithin muß die Funktion A durch jede in F aufgehende Primfunktion nach dem Modul p teilbar sein (C. 5 und 6). Multipliziert man ferner die obige Gleichung, welcher die Zahl $A(\theta)$ genügt, mit $B(\theta)^s$, und bedenkt, daß $A(\theta)\,B(\theta) = pM(\theta)$ ist, so erhält man

$$M(\theta)^s + h_1 M(\theta)^{s-1} B(\theta) + h_2 M(\theta)^{s-2} B(\theta)^2 + \cdots + h_s B(\theta)^s = 0,$$

und hieraus eine Identität von der Form

$$M^s + h_1 M^{s-1} B + h_2 M^{s-2} B^2 + \cdots + h_s B^s = FH;$$

da nun $F \equiv 0 \pmod{p, B}$, so ergibt sich

$$M^s \equiv 0 \pmod{p, B},$$

und folglich ist die Funktion M durch jede in B aufgehende Primfunktion teilbar nach dem Modul p. Oben ist aber gezeigt, daß B keine Konstante ist, mithin gibt es wenigstens eine in B aufgehende

*) In ähnlicher Weise kann man leicht zeigen, daß das Kriterium für die Teilbarkeit einer Zahl $\varphi(\theta)$ durch p in der Kongruenz $\varphi(t) \equiv 0 \pmod{p, K}$ besteht, wo K einen völlig bestimmten Teiler der Funktion F nach dem Modul p bedeutet.

Primfunktion P, und diese muß folglich auch in M aufgehen. Da ferner P in F aufgeht, weil F durch B teilbar ist, und da oben gezeigt ist, daß jede in F aufgehende Primfunktion auch in A aufgeht, so geht P ebenfalls in A auf, und folglich ist F teilbar durch P^2, weil $F \equiv A\,B \pmod{p}$ ist. Wir haben mithin wirklich gezeigt, daß es eine in M aufgehende Primfunktion P gibt, deren Quadrat zugleich in F aufgeht, w. z. b. w.

Durch die Sätze II und III ist nun in der Tat die Entscheidung der Frage, ob der Index k der Zahl θ durch die Primzahl p teilbar ist, vollständig zurückgeführt auf die Zerlegung

$$F = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} - p\,M,$$

durch welche die Funktion F als Produkt von lauter Primfunktionen nach dem Modul p dargestellt wird. Zeigt es sich, daß F durch kein Quadrat einer Primfunktion teilbar ist, daß also alle Exponenten $e_1, e_2 \cdots e_m = 1$ sind*), oder zeigt es sich, daß keine derjenigen Primfunktionen, deren Quadrate in F aufgehen, in M aufgeht, so ist k nicht durch p teilbar, und es gilt der Satz I des § 2. Gibt es aber eine in M aufgehende Primfunktion, deren Quadrat zugleich in F aufgeht, so ist k teilbar durch p, und aus dem zweiten Beweise des Satzes II geht leicht hervor, daß dann die Zerlegung des Ideals $\mathfrak{o}\,p$ in Primfaktoren eine andere ist, als die im Satz I behauptete.

Diesem Resultat fügen wir noch folgende Bemerkung hinzu. Sind die Funktionen $R_1, R_2 \cdots R_m$ resp. kongruent den Funktionen $P_1, P_2 \cdots P_m$, so sind sie ebenfalls Primfunktionen, und es wird

$$F = R_1^{e_1} R_2^{e_2} \cdots R_m^{e_m} - p\,N,$$

wo die Funktion N durchaus nicht $\equiv M \pmod{p}$ zu sein braucht. Da aber die Teilbarkeit des Index k der Zahl θ durch p von dieser Auswahl der Primfunktionen gänzlich unabhängig ist, so muß man schließen, daß die Eigenschaft der Funktion M, welche für diese Frage allein entscheidend ist, auch für jede Funktion N bestehen bleibt. Dies ließe sich leicht durch die Rechnung unmittelbar bestätigen; bezeichnet man mit Q das Produkt aller derjenigen in F aufgehenden Primfunktionen, deren Quadrate in F nicht aufgehen, so kann man durch geeignete Wahl der Funktionen $R_1, R_2 \cdots R_m$ stets zu einer Funktion N gelangen, die relative Primfunktion zu Q

*) Dies wird stets und nur dann der Fall sein, wenn die Diskriminante $\Delta(1, \theta, \theta^2 \cdots \theta^{n-1})$ der Gleichung $F(\theta) = 0$ nicht durch p teilbar ist.

ist; aber sobald M durch eine Primfunktion P teilbar ist, deren Quadrat in F aufgeht, so zeigt die Rechnung, daß auch jede Funktion N durch P teilbar ist*).

§ 4.

In den zuerst von Kummer behandelten Zahlengebieten o, welche aus einer primitiven Wurzel θ der Gleichung $\theta^m = 1$ entspringen, tritt der glückliche Umstand auf, daß die Potenzen $1, \theta, \theta^2 \dots \theta^{n-1}$, wo $n = \varphi(m)$, eine Basis des Gebietes o bilden, und daß folglich der Index k der Zahl θ, welche der ganzen Untersuchung zugrunde gelegt wird, stets $= 1$ ist. Bei der allgemeinen Untersuchung eines beliebigen endlichen Körpers Ω und des Gebietes o, welches aus allen in Ω enthaltenen ganzen Zahlen besteht, erkannte ich zwar sehr bald, daß derselbe einfache Fall nur ausnahmeweise auftritt, aber ich hielt es doch lange Zeit für sehr wahrscheinlich, daß für jede gegebene Primzahl p sich eine ganze Zahl θ des Körpers Ω würde finden lassen, deren Index nicht durch p teilbar wäre, und mit deren Hilfe es folglich gelingen würde, die Bestimmung der Idealfaktoren von p auf die Theorie der höheren Kongruenzen zurückzuführen. Da aber alle meine Versuche, die Existenz einer solchen Zahl θ nachzuweisen, fruchtlos blieben, so entschloß ich mich endlich, wo möglich die Unrichtigkeit dieser Vermutung darzutun, und zu diesem Ziele gelangte ich, wie ich schon in den Göttingischen gelehrten Anzeigen vom 20. September 1871 angedeutet

*) Hiernach beschränkt sich die Idealtheorie von Zolotareff auf den Fall, daß der Index k nicht durch p teilbar ist. Dies scheint wenigstens aus folgenden Worten hervorzugehen, welche sich in der oben erwähnten Anzeige finden (Jahrbuch über die Fortschritte der Mathematik, Bd. 6): „Um die Theorie in ihrer einfachsten Gestalt darzustellen, nimmt der Verfasser an, daß $F_1(x)$ durch keine der Funktionen V, V_1, $V_2 \cdots$ teilbar ist. Ist diese Bedingung nicht erfüllt, so kann man für einen gegebenen Modul p die Gleichung $F(x) = 0$ derart transformieren, daß jene Annahme erfüllt ist. Die Auseinandersetzung jener Transformation behält sich der Verfasser für eine andere Gelegenheit vor.“ — Da es nach meinen Untersuchungen (vgl. § 5 dieser Abhandlung) Körper gibt, in welchen die Indizes aller ganzen Zahlen θ durch dieselbe Primzahl p teilbar sind, und folglich auch alle Gleichungen $F(\theta) = 0$ diejenige störende Eigenschaft besitzen, welche sich der unmittelbaren Anwendung der Theorie von Zolotareff widersetzt, so vermute ich, daß in den eben zitierten Worten der Anzeige ein Mißverständnis obwaltet. Wahrscheinlich wird die von dem Verfasser beabsichtigte Vervollständigung seiner Theorie sich auf ähnliche Betrachtungen stützen, wie diejenigen, welche in der Theorie der idealen Zahlen von Selling entwickelt sind (Schlömilchs Zeitschrift, Bd. 10, S. 12 ff.).

habe, durch die Betrachtungen, welche den Gegenstand dieses und des folgenden Paragraphen bilden.

Es sei p eine bestimmte Primzahl, und $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ seien die sämtlichen voneinander verschiedenen Primideale, welche in p aufgehen; ihre Grade wollen wir mit $f_1, f_2 \cdots f_m$ bezeichnen, so daß z. B. $N(\mathfrak{p}_1) = p^{f_1}$ ist. Existiert nun eine ganze Zahl θ in Ω, deren Index k nicht durch p teilbar ist, so folgt aus dem Satze I in § 2, daß es in bezug auf den Modul p auch m inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ gibt, deren Grade resp. gleich $f_1, f_2 \cdots f_m$ sind. Es ist nun von der größten Wichtigkeit für unsere Untersuchung, daß diese Folgerung sich umkehren läßt, daß also folgender Satz besteht:

IV. Sind $f_1, f_2 \cdots f_m$ die Grade der sämtlichen verschiedenen, in der Primzahl p aufgehenden Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$, und gibt es m nach dem Modul p inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ resp. vom Grade $f_1, f_2 \cdots f_m$, so existiert in Ω eine ganze Zahl θ, deren Index k nicht durch p teilbar ist.

Dem Beweise dieses Satzes schicken wir aber zunächst einige Betrachtungen voraus, welche zum Teil von den Voraussetzungen desselben unabhängig sind.

Es sei $\mathfrak{p}$ irgend ein in p aufgehendes Primideal vom Grade f, so genügen (D. § 163; B. § 28, 3°) alle ganzen Zahlen ω des Körpers Ω der Kongruenz

$$\omega^{p^f} - \omega \equiv 0 \pmod{\mathfrak{p}};$$

bedeutet nun t wieder eine Variable, so ist die Funktion

$$t^{p^f} - t$$

nach dem Modul p kongruent dem Produkte aus allen inkongruenten Primfunktionen, deren Grade Divisoren der Zahl f sind (C. 19); unter diesen wähle man nach Belieben eine solche Primfunktion P, deren Grad $= f$ ist; dies ist stets möglich, da es immer mindestens eine solche Funktion gibt (C. 20). Da nun

$$t^{p^f} - t \equiv P(t)\, H(t) \pmod{p},$$

also auch

$$\omega^{p^f} - \omega \equiv P(\omega)\, H(\omega) \pmod{p},$$

und da p durch $\mathfrak{p}$ teilbar ist, so folgt, daß jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$P(\omega)\, H(\omega) \equiv 0 \pmod{\mathfrak{p}}$$

genügt; mithin ist die Anzahl ihrer nach $\mathfrak{p}$ inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p^f$, also genau so groß, wie ihr Grad. Durch

dieselben einfachen Schlüsse, welche in der rationalen Zahlentheorie zu einem ähnlichen Zwecke angewendet werden (D. § 26), kann man nun leicht beweisen, was ich der Kürze halber hier übergehe, daß in dem Zahlengebiete o eine Kongruenz r^{ten} Grades, deren Modul ein Primideal dieses Gebietes ist, niemals mehr als r inkongruente Wurzeln haben kann, und hieraus folgt für unseren Fall, daß die Kongruenz $H(\omega) \equiv 0 \pmod{\mathfrak{p}}$ höchstens $(p' - f)$ inkongruente Wurzeln besitzt, und daß folglich die Repräsentanten ω der f übrigen Zahlklassen notwendig der Kongruenz $P(\omega) \equiv 0 \pmod{\mathfrak{p}}$ genügen müssen. Für unseren Zweck reicht aber schon die Gewißheit aus, daß diese Kongruenz wenigstens eine Wurzel hat. Es sei α eine bestimmte solche Wurzel, also

$$P(\alpha) \equiv 0 \pmod{\mathfrak{p}};$$

wir betrachten nun alle Zahlen von der Form $\varphi(\alpha)$ und wollen beweisen, daß die Kongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, wenn also

$$\varphi(t) \equiv P(t)\,\psi(t) \pmod{p}$$

ist, so folgt auch

$$\varphi(\alpha) \equiv P(\alpha)\,\psi(\alpha) \pmod{p},$$

und da die beiden Zahlen p und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist auch $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$; ist aber zweitens $\varphi(t)$ nicht teilbar durch die Primfunktion $P(t)$, so sind $\varphi(t)$ und $P(t)$ relative Primfunktionen, und folglich existieren zwei Funktionen $\varphi_1(t)$, $\varphi_2(t)$, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + P(t)\,\varphi_2(t) \equiv 1 \pmod{p}$$

genügen (C. 5); dann ist auch

$$\varphi(\alpha)\,\varphi_1(\alpha) + P(\alpha)\,\varphi_2(\alpha) \equiv 1 \pmod{p},$$

und da p und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist

$$\varphi(\alpha)\,\varphi_1(\alpha) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist in diesem Falle $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}}$. Hiermit ist unsere obige Behauptung vollständig bewiesen.

Für den Fall, daß p durch $\mathfrak{p}^2$ teilbar ist, wollen wir ferner die Wurzel α der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ so wählen, daß die Zahl $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar wird. Dies ist stets möglich; ist

nämlich α eine Wurzel der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}^2}$, so wähle man nach Belieben eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl λ, und setze $\alpha' = \alpha + \lambda$, so ist

$P(\alpha') = P(\alpha) + \lambda P'(\alpha) + \lambda^2 P''(\alpha) + \cdots \equiv \lambda P'(\alpha) \pmod{\mathfrak{p}^2}$ [*)]; da nun die derivierte Funktion $P'(t)$ den Grad $(f-1)$ hat und nicht $\equiv 0 \pmod{p}$ ist, so kann sie auch nicht $\equiv 0 \pmod{p, P}$ sein, und folglich ist nach dem obigen die Zahl $P'(\alpha)$ nicht teilbar durch $\mathfrak{p}$; mithin ist das Produkt $\lambda P'(\alpha)$, und folglich auch die Zahl $P(\alpha')$ wohl teilbar durch $\mathfrak{p}$, aber nicht teilbar durch $\mathfrak{p}^2$. Nachdem so die Existenz einer solchen Zahl α' bewiesen ist, lassen wir den Akzent wieder weg, und nehmen also an, daß $P(\alpha)$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist.

Ist nun $\mathfrak{p}^e$ die höchste in p aufgehende Potenz des Primideals $\mathfrak{p}$, so wollen wir beweisen, daß die Zahlenkongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P^e}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, so ist

$$\varphi(t) \equiv P(t)^e \psi(t) \pmod{p},$$

also auch

$$\varphi(\alpha) \equiv P(\alpha)^e \psi(\alpha) \pmod{p},$$

und da beide Zahlen p und $P(\alpha)^e$ durch $\mathfrak{p}^e$ teilbar sind, so folgt $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$; wenn dagegen die Funktionenkongruenz nicht stattfindet, so ist der größte gemeinschaftliche Teiler, welchen die Funktionen $\varphi(t)$ und $P(t)^e$ nach dem Modul p haben, von der Form $P(t)^s$, wo $s < e$; bestimmt man die Funktionen $\varphi_1(t)$, $\varphi_2(t)$ so, daß

$$\varphi(t)\varphi_1(t) + P(t)^e \varphi_2(t) \equiv P(t)^s \pmod{p}$$

wird (C. 4), und bedenkt, daß p und $P(\alpha)^s$ durch $\mathfrak{p}^e$ teilbar sind, so ergibt sich

$$\varphi(\alpha)\varphi_1(\alpha) \equiv P(\alpha)^s \pmod{\mathfrak{p}^e};$$

da nun $s < e$, und $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar ist, so ist $P(\alpha)^s$ nicht teilbar durch $\mathfrak{p}^e$, und folglich ist auch $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}^e}$. Unsere Behauptung ist daher erwiesen.

Man verfahre nun mit jedem der in p aufgehenden verschiedenen Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ so, wie es im vorhergehenden beschrieben

---

[*) Durch ein Versehen schreibt Dedekind $P''(\alpha)$ statt $\frac{P''(\alpha)}{2!}$; die Zahlen $\frac{P''(\alpha)}{2!}$, $\frac{P'''(\alpha)}{3!}$, $\cdots$ sind aber auch alle ganz.]

ist, d. h. man wähle nach Belieben m Primfunktionen $P_1, P_2 \cdots P_m$, welche resp. dieselben Grade $f_1, f_2 \cdots f_m$ haben, wie jene Primideale, und bestimme ebenso viele Zahlen $\alpha_1, \alpha_2 \cdots \alpha_m$ der Art, daß $P_1(\alpha_1)$, $P_2(\alpha_2) \cdots P_m(\alpha_m)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar werden, mit der eventuellen Beschränkung, daß eine solche Zahl $P_r(\alpha_r)$ nicht durch $\mathfrak{p}_r^2$ teilbar sein darf, falls p durch $\mathfrak{p}_r^2$ teilbar ist. Da nun die Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschieden, und ihre Quadrate folglich relative Primideale sind, so kann man stets eine Zahl θ so bestimmen, daß

$$\begin{aligned} \theta &\equiv \alpha_1 \pmod{\mathfrak{p}_1^2} \\ \theta &\equiv \alpha_2 \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots \\ \theta &\equiv \alpha_m \pmod{\mathfrak{p}_m^2} \end{aligned}$$

wird (D. § 163; B. § 26); da hieraus

$$\begin{aligned} P_1(\theta) &\equiv P_1(\alpha_1) \pmod{\mathfrak{p}_1^2} \\ P_2(\theta) &\equiv P_2(\alpha_2) \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots\cdots \\ P_m(\theta) &\equiv P_m(\alpha_m) \pmod{\mathfrak{p}_m^2} \end{aligned}$$

folgt, so ergibt sich, daß die Zahlen $P_1(\theta), P_2(\theta) \cdots P_m(\theta)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar sind, daß aber, falls p durch $\mathfrak{p}_r^2$ teilbar ist, die Zahl $P_r(\theta)$ nicht durch $\mathfrak{p}_r^2$ teilbar ist. Die Zahl θ vereinigt daher in sich alle diejenigen Eigenschaften in bezug auf die sämtlichen m Primideale, welche einer jeden Zahl α_r in bezug auf das ihr korrespondierende Primideal $\mathfrak{p}_r$ zukommen. Ist daher

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

also, wie aus der Bildung der Norm hervorgeht,

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m,$$

so ist eine Zahl von der Form $\varphi(\theta)$ stets und nur dann durch eine der Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar, wenn die ihr entsprechende Funktionenkongruenz

$$\begin{aligned} \varphi(t) &\equiv 0 \pmod{p, P_1^{e_1}} \\ \varphi(t) &\equiv 0 \pmod{p, P_2^{e_2}} \\ &\cdots\cdots\cdots\cdots \\ \varphi(t) &\equiv 0 \pmod{p, P_m^{e_m}} \end{aligned}$$

stattfindet; da ferner eine ganze Zahl des Körpers stets und nur dann durch p teilbar ist, wenn sie durch jede der m Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar ist, so leuchtet ein, daß die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend ist mit dem System der m vorstehenden Funktionenkongruenzen.

Bis hierher haben wir absichtlich über die Wahl der Primfunktionen $P_1, P_2 \cdots P_m$ nichts anderes festgesetzt, als daß ihre Grade resp. mit denen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ übereinstimmen sollen, und es war z. B., falls $f_1 = f_2$, nicht ausgeschlossen, $P_1 = P_2$ zu wählen. Wir wollen jetzt die besondere Annahme unseres Satzes hinzufügen, welche darin besteht, daß es m untereinander inkongruente Primfunktionen von den vorgeschriebenen Graden gibt, und wir wollen unter $P_1, P_2 \cdots P_m$ solche inkongruente Primfunktionen verstehen. Dann sind die Potenzen $P_1^{e_1}, P_2^{e_2} \cdots P_m^{e_m}$ relative Primfunktionen, und wenn man ihr Produkt

$$P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} = R$$

setzt, so ist (C. 5) das System der m obigen Funktionenkongruenzen, und folglich auch die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend mit der einzigen Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, R}.$$

Da ferner der Grad des Produktes R gleich

$$e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

und folglich $= n$ ist, so kann eine Zahl

$$\varphi(\theta) = x_0 + x_1 \theta + x_2 \theta^2 + \cdots + x_{n-1} \theta^{n-1}$$

nur dann durch p teilbar sein, wenn

$$\varphi(t) \equiv 0 \pmod{p},$$

d. h. wenn alle n Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ durch p teilbar sind. Der Index k der Zahl θ ist folglich (nach § 1) nicht teilbar durch p. Hiermit ist unser obiger Satz bewiesen, und wir fügen nur noch die folgende Bemerkung hinzu.

Da k nicht teilbar durch p ist, so ist k auch von 0 verschieden, und folglich ist die gefundene Zahl θ die Wurzel einer irreduktiblen Gleichung $F(\theta) = 0$ vom n^{ten} Grade; da nun $F(\theta) \equiv 0 \pmod{p}$, so muß die Funktion F durch R teilbar sein nach dem Modul p; da ferner beide Funktionen denselben Grad n und denselben höchsten Koeffizienten 1 haben, so muß $F \equiv R \pmod{p}$, d. h.

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

sein, und hiermit sind wir zum Ausgangspunkt unserer Untersuchung in § 2 zurückgekehrt.

§ 5.

Die letzte Untersuchung hat uns ein Kriterium geliefert, durch welches die Frage entschieden wird, ob es wirklich in Ω eine ganze Zahl θ gibt, deren Index durch eine gegebene Primzahl p nicht teilbar ist. Wenn

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_m^{e_m}$$

ist, wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ verschiedene Primideale resp. von den Graden $f_1, f_2 \cdots f_m$ bedeuten, so wird der singuläre Fall, daß die Indizes aller in Ω enthaltenen ganzen Zahlen durch p teilbar sind, jedesmal und nur dann eintreten, wenn es unmöglich ist, m nach dem Modul p inkongruente Primfunktionen von den Graden $f_1, f_2 \cdots f_m$ aufzustellen. Es fragt sich daher nur noch, ob diese Erscheinung, daß nicht genug Primfunktionen existieren, wirklich jemals auftreten kann. Um hierüber zu entscheiden, wollen wir den denkbar einfachsten Versuch anstellen. Die inkongruenten Primfunktionen ersten Grades sind die folgenden

$$t,\ t+1,\ t+2 \cdots t+(p-1),$$

ihre Anzahl ist $= p$; der obige singuläre Fall wird daher gewiß in einem Körper Ω eintreten, in welchem die Primzahl p durch mindestens $(p+1)$ verschiedene Primideale ersten Grades teilbar ist; da aber, wie aus der Betrachtung der Normen hervorgeht, das Ideal $\mathfrak{o}\,p$ ein Produkt von höchstens n Primidealen ist, so muß der Grad n eines solchen Körpers mindestens $= p+1$ sein. Nimmt man, um den einfachsten Fall zu erhalten, die kleinste Primzahl $p = 2$, so entsteht also die Frage, ob es kubische Körper Ω gibt, in welchen die Zahl 2 durch drei verschiedene Primideale ersten Grades teilbar ist; in einem solchen Körper würden die Indizes aller ganzen Zahlen gerade sein. Diese Untersuchung ist in den Göttingischen gelehrten Anzeigen vom 20. September 1871 in voller Allgemeinheit angestellt, und sie hat zu einer bejahenden Antwort geführt; hier will ich mich begnügen, ein einziges, auch dort schon angeführtes Beispiel mitzuteilen [*)].

[*) Die eben erwähnte Anzeige enthält auch eine Ausführung über die Methode, wodurch Dedekind auf das hier behandelte Beispiel gekommen ist. Weiter wird ein anderes Beispiel eines Körpers mit gemeinsamen Indexteilern gegeben, nämlich ein Körper vierten Grades, worin die Primzahl 2 in zwei Primideale zweiten Grades zerfällt.]

Es sei α eine Wurzel der irreduktiblen Gleichung dritten Grades

$$F(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 8 = 0;$$

um ihre Diskriminante zu finden, betrachten wir die Zahl

$$F'(\alpha) = \delta = -2 - 2\alpha + 3\alpha^2$$

und bilden sukzessive, unter Zuziehung von $F(\alpha) = 0$, die Produkte

$$\begin{aligned} \delta\alpha &= 24 + 4\alpha + \alpha^2 \\ \delta\alpha^2 &= 8 + 26\alpha + 5\alpha^2; \end{aligned}$$

durch lineare Elimination von 1, α, α^2 aus diesen drei Gleichungen erhält man

$$\begin{vmatrix} -2-\delta, & -2 & , & 3 \\ 24 & , & 4-\delta, & 1 \\ 8 & , & 26 & , & 5-\delta \end{vmatrix} = 0,$$

d. h.

$$\delta^3 - 7\delta^2 - 2012 = 0,$$

und folglich ist die Diskriminante

$$\Delta(1, \alpha, \alpha^2) = -N(\delta) = -2012 = -2^2 \cdot 503.$$

Da 503 eine Primzahl ist, so gehen in dieser Diskriminante nur die beiden Quadrate 1 und 4 auf, und folglich ist der Index k der Zahl α entweder $= 1$, oder $= 2$; es ist daher die Funktion

$$F(t) = t^3 - t^2 - 2t - 8$$

nur in bezug auf den Modul $p = 2$ zu untersuchen. Offenbar ist

$$F = P_1^2 P_2 - 2M \equiv P_1^2 P_2 \pmod 2,$$

wo

$$P_1 = t, \quad P_2 = t - 1, \quad M = t + 4;$$

da nun gleichzeitig P_1 in M, und P_1^2 in F aufgeht nach dem Modul 2, so muß (nach dem zweiten Beweise des Satzes II in § 3) die Zahl

$$P_1(\alpha)\, P_2(\alpha) = \alpha(\alpha - 1)$$

durch 2 teilbar, und folglich $k = 2$ sein. Dies wird sich sofort dadurch bestätigen, daß die Zahl

$$\beta = \tfrac{1}{2}\alpha(\alpha - 1) - 1$$

sich ebenfalls als eine ganze Zahl erweist; in der Tat, man erhält mit Rücksicht auf $F(\alpha) = 0$ die Gleichungen

$$\begin{aligned} \alpha^2 &= 2 + \alpha + 2\beta \\ \beta^2 &= -2 + 2\alpha - \beta \\ \alpha\beta &= 4 \end{aligned}$$

und hieraus

$$\beta^3 + \beta^2 + 2\beta - 8 = 0.$$

Da ferner

$$1 = 1\cdot 1 + 0\cdot\alpha + 0\cdot\beta$$
$$\alpha = 0\cdot 1 + 1\cdot\alpha + 0\cdot\beta$$
$$\alpha^2 = 2\cdot 1 + 1\cdot\alpha + 2\cdot\beta,$$

so ist

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 2, & 1, & 2 \end{vmatrix}^2 \Delta(1, \alpha, \beta) = 2^2\,\Delta(1, \alpha, \beta),$$

also

$$\Delta(1, \alpha, \beta) = -503,$$

und da diese Zahl durch kein Quadrat (außer 1) teilbar ist, so ist sie die Grundzahl D unseres kubischen Körpers Ω, und die Zahlen $1, \alpha, \beta$ bilden eine Basis des aus allen ganzen Zahlen ω dieses Körpers Ω bestehenden Gebiets $\mathfrak{o}$, d. h. nach der schon mehrfach gebrauchten Bezeichnung, es ist

$$\mathfrak{o} = [1, \alpha, \beta];$$

jede solche ganze Zahl, d. h. jede in $\mathfrak{o}$ enthaltene Zahl ω ist von der Form

$$\omega = z + x\alpha + y\beta,$$

wo z, x, y willkürliche ganze rationale Zahlen bedeuten.

Wir wollen nun auf Grund dieses Resultats die Idealfaktoren der Zahl 2 bestimmen. Da

$$\left.\begin{aligned} \alpha^2 &= \quad 2 + \alpha + 2\beta \equiv \alpha \\ \beta^2 &= -2 + 2\alpha - \beta \equiv \beta \end{aligned}\right\} \pmod 2,$$

so folgt allgemein

$$(z + x\alpha + y\beta)^2 \equiv z^2 + x^2\alpha^2 + y^2\beta^2 \equiv z + x\alpha + y\beta \pmod 2,$$

d. h. jede Zahl ω des Gebietes $\mathfrak{o}$ genügt der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod 2.$$

Hieraus folgt zunächst, daß die Zahl 2 durch kein Quadrat eines Primideals teilbar sein kann; wäre nämlich $\mathfrak{o}(2) = \mathfrak{p}^2\mathfrak{q}$, wo $\mathfrak{p}$ ein Primideal oder wenigstens ein von $\mathfrak{o}$ verschiedenes Ideal bedeutet, so würde, da $\mathfrak{p}\mathfrak{q}$ nicht durch $\mathfrak{o}(2)$ teilbar ist, eine Zahl ω existieren, welche durch $\mathfrak{p}\mathfrak{q}$, aber nicht durch 2 teilbar wäre; dann wäre aber ω^2 teilbar durch $\mathfrak{p}^2\mathfrak{q}^2$, also auch durch 2, und dies widerspricht der vorstehenden Kongruenz $\omega^2 \equiv \omega \pmod 2$. Mithin ist $\mathfrak{o}(2)$ entweder ein Primideal oder ein Produkt aus lauter verschiedenen Primidealen. Es sei $\mathfrak{p}$ irgend ein in 2 aufgehendes Primideal, so genügt jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod{\mathfrak{p}},$$

und folglich ist die Anzahl ihrer inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$; da diese Anzahl aber niemals größer als der Grad der Kongruenz sein kann, so ergibt sich $N(\mathfrak{p}) \leqq 2$, und folglich $N(\mathfrak{p}) = 2$, weil $\mathfrak{p}$ ein Primideal, also von $\mathfrak{o}$ verschieden, mithin $N(\mathfrak{p}) > 1$ ist. Jedes in 2 aufgehende Primideal ist daher vom ersten Grade, und folglich muß, da $N(2) = 2^3 = 8$ ist,

$$\mathfrak{o}(2) = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}$$

sein, wo $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ drei voneinander verschiedene Primideale ersten Grades bedeuten. Hiermit ist das Auftreten der erwähnten singulären Erscheinung erwiesen, und es muß sich bestätigen, daß die Indizes aller Zahlen ω durch 2 teilbar sind. In der Tat, setzt man

$$z' = z^2 + 2x^2 - 2y^2 + 8xy$$
$$x' = x^2 + 2y^2 + 2xz$$
$$y' = 2x^2 - y^2 + 2yz,$$

so ist

$$\omega^2 = z' + x'\alpha + y'\beta,$$

und der Index der Zahl ω ist gleich der Determinante

$$\begin{vmatrix} 1, & 0, & 0 \\ z, & x, & y \\ z', & x', & y' \end{vmatrix} = xy' - yx' = 2x^3 - x^2y - xy^2 - 2y^3,$$

welche offenbar stets eine gerade Zahl ist.

Um unser Beispiel ganz zu vollenden, und um die aus der allgemeinen Theorie geschöpften Voraussagungen auch durch die Rechnung zu bestätigen, wollen wir endlich zur Darstellung der hier auftretenden Ideale in Form von endlichen, dreigliedrigen Moduln (D. § 161; B. § 3), d. h. zur Bestimmung dieser Ideale durch ihre Basiszahlen schreiten. Diese Darstellungen sind die folgenden

$$\mathfrak{a} = [2, \alpha, 1 + \beta]$$
$$\mathfrak{b} = [2, 1 + \alpha, \beta]$$
$$\mathfrak{c} = [2, \alpha, \beta].$$

Das System $\mathfrak{a}$ aller Zahlen von der Form

$$\alpha' = 2z + \alpha x + (1 + \beta)y,$$

wo z, x, y willkürliche ganze rationale Zahlen bedeuten, besitzt in der Tat die beiden fundamentalen Eigenschaften eines Ideals, nämlich:

I. Die Summen und Differenzen von je zwei Zahlen α' des Systems $\mathfrak{a}$ gehören demselben System $\mathfrak{a}$ an.

II. Jedes Produkt aus einer Zahl α' des Systems $\mathfrak{a}$ und aus einer Zahl ω des Gebiets $\mathfrak{o}$ ist wieder eine Zahl des Systems $\mathfrak{a}$.

Die erste Eigenschaft ist evident, und um die zweite nachzuweisen, genügt es, darzutun, daß die Produkte aus je einer der Basiszahlen 2, α, $(1+\beta)$ von $\mathfrak{a}$ und je einer der Basiszahlen 1, α, β von $\mathfrak{o}$ sämtlich in $\mathfrak{a}$ enthalten sind; dies ist unmittelbar evident für die fünf Produkte

$$2\cdot 1,\ \alpha\cdot 1,\ (1+\beta)\cdot 1,\ 2\cdot\alpha,\ 2\cdot\beta = -2+2(1+\beta),$$

und für die übrigen vier ergibt sich dasselbe aus den Gleichungen

$$\alpha\cdot\alpha = \alpha+2(1+\beta), \qquad \alpha\cdot\beta = 2\cdot 2,$$
$$(1+\beta)\alpha = 2\cdot 2+\alpha, \qquad (1+\beta)\beta = -2+2\alpha.$$

Ebenso wird bewiesen, daß die Systeme $\mathfrak{b}$ und $\mathfrak{c}$ Ideale sind.

Die Norm $N(\mathfrak{m})$ eines Ideals $\mathfrak{m}$ ist die Anzahl $(\mathfrak{o}, \mathfrak{m})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ inkongruenten Zahlen (D. § 163; B. § 20), und diese Anzahl ist gleich der Determinante der Ausdrücke, welche in bezug auf die Basiszahlen von $\mathfrak{o}$ linear sind und die Basiszahlen von $\mathfrak{m}$ darstellen (D. § 161; B. § 4, 4°). Es ist daher z. B.

$$N(\mathfrak{a}) = \begin{vmatrix} 2, & 0, & 0 \\ 0, & 1, & 0 \\ 1, & 0, & 1 \end{vmatrix} = 2,$$

und ebenso ergibt sich

$$N(\mathfrak{b}) = N(\mathfrak{c}) = 2.$$

Wenn aber die Norm eines Ideals eine Primzahl ist, so muß das Ideal notwendig ein Primideal sein, weil allgemein $N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2)$ ist; mithin sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Primideale. Sie sind ferner verschieden voneinander, weil die in $\mathfrak{b}$ und in $\mathfrak{c}$ enthaltene Zahl β nicht in $\mathfrak{a}$ enthalten, und weil die in $\mathfrak{c}$ enthaltene Zahl α nicht in $\mathfrak{b}$ enthalten ist. Es muß folglich die in allen drei Idealen enthaltene Zahl 2 auch in dem Produkte $\mathfrak{a}\mathfrak{b}\mathfrak{c}$ enthalten sein; mithin ist $\mathfrak{o}(2) = \mathfrak{m}\mathfrak{a}\mathfrak{b}\mathfrak{c}$, wo $\mathfrak{m}$ ein Ideal bedeutet; nimmt man aber die Norm, so ergibt sich

$$N(2) = 8 = N(\mathfrak{m})N(\mathfrak{a})N(\mathfrak{b})N(\mathfrak{c}) = 8N(\mathfrak{m});$$

mithin ist $N(\mathfrak{m}) = 1$, also $\mathfrak{m} = \mathfrak{o}$, und $\mathfrak{o}(2) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$. Aber auch dieses, aus allgemeinen Sätzen geschlossene Resultat wollen wir durch die eigentliche Rechnung, d. h. durch die wirkliche Ausführung der Multiplikation der Ideale bestätigen (D. § 165; B. § 12).

Unter dem Produkte $\mathfrak{a}\mathfrak{b}$ zweier Ideale wird das System aller Produkte $\alpha'\beta'$ und aller Summen von solchen Produkten $\alpha'\beta'$ verstanden, wo α', β' beliebige Zahlen resp. der Ideale $\mathfrak{a}$, $\mathfrak{b}$ bedeuten

(D. § 163; B. § 22). Ein solches Produkt erscheint daher zunächst als ein endlicher Modul, dessen Basiszahlen die sämtlichen Produkte aus je einer Basiszahl von $\mathfrak{a}$ und je einer Basiszahl von $\mathfrak{b}$ sind. In unserem Falle ist daher $\mathfrak{a}\mathfrak{b}$ der endliche Modul, dessen Basiszahlen die neun Produkte

$$2\cdot 2 = 4, \quad 2(1+\alpha) = 2+2\alpha, \quad 2\cdot\beta = 2\beta,$$
$$\alpha\cdot 2 = 2\alpha, \quad \alpha(1+\alpha) = 2+2\alpha+2\beta, \quad \alpha\beta = 4,$$
$$(1+\beta)\cdot 2 = 2+2\beta, \quad (1+\beta)(1+\alpha) = 5+\alpha+\beta,$$
$$(1+\beta)\beta = -2+2\alpha$$

sind; da aber von diesen neun Zahlen nur drei voneinander unabhängig sind (D. § 159; B. § 4), so ist die von mir ausführlich beschriebene Methode (B. § 4, 6°) anzuwenden, um diesen neungliedrigen Modul auf einen dreigliedrigen zurückzuführen; durch die Ausführung dieser sehr einfachen und leichten Rechnung erhält man die eine der sechs folgenden Gleichungen:

$$\mathfrak{a}^2 = [4, \quad \alpha, \quad 3+\beta]; \quad \mathfrak{b}\mathfrak{c} = [2, \ 2\alpha, \quad \beta]$$
$$\mathfrak{b}^2 = [4, \ 1+\alpha, \quad \beta]; \quad \mathfrak{c}\mathfrak{a} = [2, \quad \alpha, \quad 2\beta]$$
$$\mathfrak{c}^2 = [4, \ 2+\alpha, \ 2+\beta]; \quad \mathfrak{a}\mathfrak{b} = [2, \ 2\alpha, \ 1+\alpha+\beta].$$

Die übrigen ergeben sich auf dieselbe Weise; und wenn man abermals nach derselben Methode mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ multipliziert, so erhält man folgende zehn Hauptideale:

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} = [2, \quad 2\alpha, \quad 2\beta \ ] = \mathfrak{o}(2)$$
$$\mathfrak{a}^2\mathfrak{c} = [4, \quad \alpha, \quad 2+2\beta] = \mathfrak{o}\alpha$$
$$\mathfrak{b}^2\mathfrak{c} = [4, \ 2+2\alpha, \quad \beta \ ] = \mathfrak{o}\beta$$
$$\mathfrak{a}\mathfrak{c}^2 = [4, \ 2+\alpha, \quad 2\beta \ ] = \mathfrak{o}(\alpha-2)$$
$$\mathfrak{b}\mathfrak{c}^2 = [4, \ 2\alpha, \quad 2+\beta \ ] = \mathfrak{o}(2-\beta)$$
$$\mathfrak{a}^2\mathfrak{b} = [4, \ 2\alpha, \quad 3+\alpha+\beta] = \mathfrak{o}(3+\alpha+\beta)$$
$$\mathfrak{a}\mathfrak{b}^2 = [4, \ 2+2\alpha, \ 1+\alpha+\beta] = \mathfrak{o}(1+\alpha+\beta)$$
$$\mathfrak{a}^3 = [8, \ 4+\alpha, \quad 3+\beta \ ] = \mathfrak{o}(3+2\alpha+\beta)$$
$$\mathfrak{b}^3 = [8, \ 1+\alpha, \quad 4+\beta \ ] = \mathfrak{o}(1+\alpha)$$
$$\mathfrak{c}^3 = [8, \ 2+\alpha, \quad 2+\beta \ ] = \mathfrak{o}(\alpha+\beta-4)$$

Die zehn Zahlen μ, welchen diese Hauptideale $\mathfrak{o}\mu = [\mu, \alpha\mu, \beta\mu]$ entsprechen, sind durch die folgenden, leicht zu verifizierenden Relationen miteinander verbunden:

$$\alpha(\alpha-2)(1+\alpha) = 2^3; \quad \alpha\beta = (\alpha-2)(1+\alpha+\beta) = 2^2$$
$$(\alpha-2)(3+\alpha+\beta) = 2^2\alpha; \quad \alpha(2-\beta) = 2(\alpha-2)$$
$$(\alpha-2)(3+2\alpha+\beta) = \alpha^2; \quad \alpha(\alpha+\beta-4) = (\alpha-2)^2.$$

Durch dieses Beispiel, welchem man viele andere an die Seite stellen könnte, ist außer Zweifel gesetzt, daß es Körper Ω gibt, in welchen die Indizes aller ganzen Zahlen durch eine und dieselbe Primzahl p teilbar sind. Dies Resultat ist in mancher Beziehung kein willkommenes. Es gibt in der Tat sehr wichtige Sätze der Idealtheorie, welche sich durch die Theorie der höheren Kongruenzen sehr leicht würden beweisen lassen, wenn der Satz I in § 2 nicht an die Voraussetzung gebunden wäre, daß der Index k der Zahl θ nicht durch p teilbar sein darf; wir haben aber jetzt gesehen, daß in manchen Fällen diese Voraussetzung auf keine Weise zu erfüllen ist, wie man auch die Zahl θ wählen mag, und hieraus geht hervor, daß solche Beweise, die sich auf den genannten Satz stützen, häufig die erforderliche Allgemeinheit nicht besitzen. Als Beispiel führe ich den folgenden, besonders wichtigen Satz an, den ich ebenfalls in den Göttingischen gelehrten Anzeigen vom 20. September 1871 zuerst ausgesprochen habe:

Die Grundzahl D eines Körpers Ω ist aus allen und nur aus denjenigen rationalen Primzahlen p zusammengesetzt, welche in diesem Körper durch das Quadrat eines Primideals teilbar sind.

Gibt es in Ω eine ganze Zahl, deren Index durch die Primzahl p nicht teilbar ist, so folgt für diese Primzahl p die Richtigkeit des Satzes augenscheinlich sehr leicht aus § 2. Aber auf diese Weise gelangt man offenbar nicht zu dem Beweise der allgemeinen Gültigkeit des Satzes, und es ist mir erst nach manchen vergeblichen Versuchen gelungen, den allgemeinen Beweis in aller Strenge zu führen. Die ausführliche Darstellung dieses Gegenstandes, bei welcher der Satz selbst noch eine wesentliche Erweiterung erfahren wird, muß ich aber für eine andere Gelegenheit mir vorbehalten.

Erläuterungen zur vorstehenden Abhandlung.

Das Problem der Verallgemeinerung der Kummerschen Theorie der Ideale in Kreisteilungskörpern auf beliebige Körper führt natürlich zu einer Definition der Ideale mittels höheren Kongruenzen. Schon Selling (Zeitschr. f. Math. u. Phys., Bd. 10, S. 17—47 (1865)) schlägt diesen Weg ein, und es gelingt ihm, zwar unter Anwendung von Galoisschen Imaginären und weiteren Hilfskörpern, eine ausnahmslose Theorie der Ideale in Galoisschen Körpern zu gewinnen. Die Primidealzerlegung einer Primzahl p wird aus der Zerlegung der definierenden Gleichung (mod. p^{α}) in diesen Hilfskörpern abgeleitet. Ein Nach-

weis der Invarianz dieser Ideale, d. h. ihre Unabhängigkeit von der gewählten Gleichung wird aber nicht gebracht.

Wie aus der Einleitung hervorgeht, hat auch Dedekind zuerst diese Methode versucht, aber wieder aufgegeben, um die Theorie der Ideale in der abstrakten Form zu schaffen, wie er sie in der zweiten Auflage von Dirichlets Zahlentheorie dargestellt hat. In dieser Form entsteht aber sofort die Frage, wie die Primidealzerlegung einer gegebenen Zahl im Körper bestimmt werden kann, und speziell wie Primideale bei gegebener, definierender Gleichung abgeleitet werden können. Diese Frage wird für Primzahlen, welche den Index nicht teilen, durch den Satz I, § 2 erledigt, aber die vollständige Lösung scheitert an dem Vorkommen der gemeinsamen Indexteiler (gemeinsame außerwesentliche Diskriminantenteiler).

In der mehrmals von Dedekind erwähnten Arbeit von Zolotareff (1874) wird umgekehrt die Primidealzerlegung durch die Zerlegung des Satzes I definiert. Wenn aber p ein Teiler des Index ist, genügt diese Definition nicht der Forderung der Invarianz. Eine ausnahmslose Theorie der Ideale gibt aber Zolotareff in der Arbeit: „Sur la théorie des nombres complexes“ (Journ. de Math., Bd. 6, S. 51—84, 129—166, 3e série (1880); man vgl. auch: Mélanges math. et astron., Bulletin de l'academie des sciences, St. Petersburg, Bd. 5, 13./25. September 1877), worin er auch eine Übersicht über seine erste Theorie gibt. Bei seiner allgemeinen Theorie der Ideale muß aber Zolotareff so wie Dedekind eine Definition der Ideale mittels der definierenden Gleichung aufgeben.

Man kann die Zolotareffsche Theorie kurz folgendermaßen beschreiben: Zuerst wird eine Methode angegeben, wodurch man in endlich vielen Schritten ein vollständiges Restsystem

$$(1) \qquad \alpha_1, \alpha_2, \ldots, \alpha_{p^n-1} \pmod{p} \text{ (die Null ausgenommen)}$$

aufstellen kann. Eine Zahl α in (1) heißt relativ prim zu p, wenn es keine Zahl γ in (1) gibt, wofür $\alpha\gamma$ durch p teilbar ist. Zwei Zahlen α und β heißen relativ prim in bezug auf p, wenn es keine Zahl γ in (1) gibt, wofür gleichzeitig $\alpha\gamma$ und $\beta\gamma$ durch p teilbar sind. Es können dann zwei Zahlen γ und δ so bestimmt werden, daß

$$\alpha\gamma + \beta\delta \equiv 1 \pmod{p},$$

und hieraus erhält man leicht eine Definition des größten gemeinsamen Teilers in bezug auf p. Die Primideale werden dann folgendermaßen eingeführt: Eine Zahl α enthält nur ein Primideal β von p, wenn jede Zahl in (1), welche nicht zu α relativ prim ist, die Zahl α als Teiler in bezug auf p enthält. Aus (1) können dann in endlich vielen Schritten die Anzahl der vorkommenden verschiedenen Primideale bestimmt werden.

Es würde hier zu weit führen, auf alle späteren Begründungen der Idealtheorie einzugehen. Es sollen hier nur ganz kurz die wichtigsten Methoden zur Bestimmung der Primideale erwähnt werden.

Die Kroneckersche Theorie der Formen (Journ. f. Math., Bd. 92, S. 1—122 (1882)) gibt eine theoretisch besonders einfache Bestimmung der Primidealzerlegung der rationalen Primzahlen. Wie zuerst in voller Allgemeinheit von Hensel (Journ. f. Math., Bd. 113, S. 61—83 (1894)) gezeigt worden ist, besteht in dieser Theorie für alle Primzahlen ein vollständiges Analogon zum Dedekindschen Satze.

Die Schwierigkeiten der gemeinsamen Indexteiler werden hier dadurch überwunden, daß man statt einer speziellen Gleichung eine Fundamentalgleichung

$F(x_1 \dots x_n) = 0$ des Körpers studiert. Wenn die Zahlen ω_i eine Minimalbasis bilden, ist $F(x_1 \dots x_n) = 0$ die Gleichung, welcher die Fundamentalform

$$\omega = \omega_1 x_1 + \cdots + \omega_n x_n \tag{2}$$

genügt. Die entsprechende Indexform ist dann eine Einheitsform, d. h. ihre Koeffizienten haben keinen gemeinsamen Teiler, und man erhält für die Fundamentalgleichung Resultate, welche dem Dedekindschen Satze I genau entsprechen.

Diese Lösung des Problems gibt aber keine Auskunft über den Zusammenhang zwischen den Eigenschaften der Gleichungen des Körpers und der Primidealzerlegung, wie es beim Dedekindschen Satze der Fall ist. In der von Hensel begründeten p-adischen Theorie der algebraischen Zahlen wird diese Lücke zum Teil ausgefüllt, indem man zeigt, daß die Zerlegung der definierenden Gleichung in irreduzible p-adische Faktoren der Zerlegung von p in Primidealpotenzen entspricht. Für die vollständige Bestimmung der Primidealzerlegung muß man aber auch hier auf die Kroneckersche Theorie zurückgreifen. (Man sehe K. Hensel: Theorie der algebraischen Zahlen I, Leipzig 1908.)

Man kann aber zeigen, daß die Schwierigkeiten der Dedekindschen Theorie dadurch vollständig beseitigt werden können, daß man statt Kongruenzen (mod. p) immer Kongruenzen (mod. p^α) betrachtet, wo α eine feste Zahl ist, und $\alpha > \delta$, wenn die Diskriminante der entsprechenden Gleichung genau durch p^δ teilbar ist. Die entsprechenden irreduziblen Faktoren sind dann zwar nicht (mod. p^α), aber doch (mod. $p^{\alpha-\delta}$) eindeutig bestimmt. Die gemeinsamen Indexteiler verlieren dadurch gänzlich ihre Ausnahmestellung und man erhält eine eindeutige Korrespondenz zwischen Primidealzerlegung und Faktoren der Gleichung (O. Ore, Math. Ann., Bd. 96, S. 315—352 (1926) und Bd. 97, S. 569—598 (1927)). Weiter kann die Dedekindsche Darstellung der Primideale in der Form $\beta = (p, \varphi(\vartheta))$ durch eine Methode bestimmt werden, welche mit der Bestimmung der Reihenentwicklung algebraischer Funktionen große Ähnlichkeit zeigt (O. Ore, Math. Ann., Bd. 99, S. 84—117 (1928)).

Die Resultate in § 4 der vorliegenden Abhandlung geben ein einfaches Kriterium für gemeinsame Indexteiler. Hensel (Journ. f. Math., Bd. 113, S. 128—160 (1894)) leitet ein weiteres Kriterium ab, indem er die Bedingung dafür aufstellt, daß die Indexform $k(x_1, \dots, x_n)$ zu (1) für alle ganzzahligen Werte der x_i einen gemeinsamen Teiler hat. Durch diese Untersuchung gelang es auch Hensel, die Kroneckersche Vermutung zu beweisen, daß für Körper mit gemeinsamen Indexteilern immer Erweiterungskörper K derart existieren, daß, wenn die Variablen x_i in (1) alle ganze Zahlen in K durchlaufen, keine gemeinsame Idealteiler der entsprechenden Werte der Indexform vorkommen können.

Das Henselsche Kriterium zeigt, daß für einen gemeinsamen Indexteiler p gleich $p < \frac{n(n-1)}{2}$ ist. E. v. Zylinsky (Math. Ann., Bd. 73, S. 273—274 (1913)) beweist unter Anwendung des Dedekindschen Kriteriums, daß sogar $p < n$ ist. M. Bauer (Math. Ann., Bd. 64, S. 573—576 (1907)) zeigt umgekehrt, daß, wenn diese Bedingung erfüllt ist, auch immer Körper n-ten Grades existieren, worin p gemeinsamer Indexteiler ist. Weiter wird die Existenz von Indexteilern mit speziellen Eigenschaften nachgewiesen. Diese Resultate folgen auch sofort aus dem allgemeinen Existenzsatz für Körper mit vorgeschriebenen Primidealzerlegungen gegebener Primzahlen (H. Hasse, Math. Ann., Bd. 95, S. 229—238 (1925); O. Ore, Math. Zeitschr., Bd. 20, S. 267—279 (1924)).

Ore.

XVI.

Sur la théorie des nombres complexes idéaux. (Extrait d'une lettre adressée à M. Hermite.)

[Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Paris, Bd. 90, S. 1205—1207 (1880).]

Je prends la liberté de vous communiquer la remarque suivante sur les théorèmes signalés par M. Sylvester dans les *Comptes rendus* des 16 et 23 février, lesquels se rapportent à quelques congruences ressortant de la théorie de la division du cercle. Comme toute la théorie des congruences est entièrement contenue dans celle des *idéaux*, les théorèmes de M. Sylvester ne sont que des conséquences très spéciales d'un seul théorème, par lequel sont définis tous les idéaux qui se rencontrent dans la théorie des nombres, composés rationnellement de racines de l'unité. Ce théorème, comme je l'ai déjà fait remarquer dans le § 27 de mon Mémoire *Sur la théorie des nombres entiers algébriques* (Paris, 1877, p. 109), se déduit facilement des résultats obtenus par M. Kummer, à l'aide de certains principes généraux dont l'exposition complète dépasserait les bornes de cette Communication; pour le moment, il suffira d'énoncer le théorème en question.

Soit θ une racine primitive de l'équation $\theta^m = 1$; l'ensemble K_m de tous les nombres $\eta = F(\theta)$ qui se déduisent de θ par les opérations rationnelles de l'Arithmétique constitue ce que j'appelle un *corps* de nombres; la théorie des idéaux de ce corps cyclotomique K_m, dont le *degré* est égal à $\varphi(m)$, a été établie par M. Kummer (*Mémoires de l'Académie de Berlin*, 1856). Prenons maintenant un nombre déterminé $\eta = F(\theta)$, et cherchons le degré n de l'équation irréductible $\psi(\eta) = 0$, dont η est la racine; pour cela, il faut considérer le système de tous les nombres entiers rationnels qui sont premiers avec m et incongrus suivant m; parmi ces nombres, dont le nombre est égal à $\varphi(m)$, il y a un système (h), comprenant tous

les exposants h, qui satisfont à la condition $F(\theta^h) = F(\theta)$ et qui forment un *groupe*, c'est-à-dire que le produit de deux quelconques d'entre eux se trouve dans le même système (h); le nombre de ces exposants h est $\frac{\varphi(m)}{n}$.

L'ensemble de tous les nombres $\omega = f(\eta)$, composés rationnellement de η, constitue un corps cyclotomique Ω de degré n, lequel est un *diviseur* du corps K_m. Réciproquement, si Ω est un corps dont tous les nombres sont contenus dans le corps K_m, il existe toujours des nombres η qui engendrent le corps Ω de la manière indiquée ci-dessus. Le corps Ω est complètement déterminé par le groupe (h), et à chaque groupe (h) correspond un corps Ω.

Après avoir rappelé ces principes bien connus de la théorie de la division du cercle, je vais maintenant proposer le théorème général sur les idéaux d'un tel corps cyclotomique Ω. En me servant des notations dont j'ai fait usage dans le Mémoire cité plus haut, je désigne par ν l'idéal principal consistant en tous les nombres *entiers* contenus dans le corps Ω. Soit p un nombre premier quelconque (rationnel, positif); on peut poser $m = m'p'$, où p' désigne la plus haute puissance de p, laquelle divise le nombre m; soit en outre $\frac{\varphi(p')}{g}$ le nombre de tous ceux, parmi les nombres h contenus dans le groupe (h), qui sont égaux à $1 \pmod{m'}$, et soit f le plus petit exposant positif qui satisfasse à la condition que p^f soit congru, suivant le module m', à l'un des nombres h du groupe (h); alors le degré n du corps Ω sera divisible par le produit fg, et, si l'on pose $n = efg$, on aura la décomposition

$$\nu p = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^g,$$

où les e idéaux premiers $\mathfrak{p}$ sont différents entre eux; le *degré* de ces idéaux est égal à f, c'est-à-dire que leur *norme* est donnée par l'équation

$$N(\mathfrak{y}) = p^f.$$

Ce théorème général revient à celui de M. Kummer pour le cas $n = \varphi(m)$.

Dans un Mémoire sur la dépendance entre la théorie des congruences et celle des idéaux (Göttingue, 1878), j'ai démontré que les équations irréductibles de degré n auxquelles satisfont les nombres entiers d'un corps quelconque Ω de degré n, prises par rapport à

un module premier p, se résolvent en facteurs irréductibles, dont les degrés coïncident, en général, avec les degrés des idéaux premiers $\mathfrak{p}$ qui divisent le nombre p. Par suite, la condition pour que ces congruences aient des racines *commensurables* [*)] consiste dans l'existence d'un tel idéal $\mathfrak{p}$ dont le degré soit égal à 1. En faisant l'application de ce fait à notre exemple, où il s'agit des équations $\psi(\eta) = 0$ de la division du cercle, on voit bien que les racines x de la congruence cyclotomique $\psi(x) \equiv 0 \pmod{p}$ ne seront commensurables que dans le cas $f = 1$, c'est-à-dire dans le cas que p soit congru, suivant le module m', à l'un des nombres h du groupe (h). Pour descendre finalement de la théorie générale aux théorèmes de M. Sylvester, il suffit d'observer que le corps Ω du degré $\frac{1}{2}\varphi(m)$, qui provient du nombre $\eta = \theta + \theta^{-1}$, correspond au groupe (h) des deux nombres $h \equiv \pm 1 \pmod{m}$[**)].

[*) D. h. im rationalen Bereiche lösbar sind.]

[**) Sylvester hat in zwei Noten [Compt. rend., Bd. 90, S. 287—289, 345—347 (1880)] gezeigt, daß dieses spezielle Polynom $\psi(x)$, abgesehen von Teilern von m, nur Primzahlteiler von der Form $p = tm \pm 1$ haben kann.]

XVII.

Réponse à une remarque de M. Sylvester concernant les Leçons sur la théorie des nombres de Dirichlet.

[Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Paris. Bd. 91, S. 154—156 (1880).]

Dans le § 47 de la *Zahlentheorie* de Dirichlet (3e éd., p. 110), où il s'agit de l'algorithme connu qui sert à déterminer la valeur du symbole $\left(\frac{b}{a}\right)$, on rencontre cette phrase: „Es zeigt sich nun, daß die damals notwendige Zerlegung in Primzahlfaktoren (abgesehen von dem Faktor 2) ganz überflüssig geworden.". Ce passage a donné lieu à la remarque suivante de M. Sylvester (*Comptes rendus* du 10 mai 1880, p. 1105): „Ce qui précède ici rend évident (il me semble) que cette exclusion du nombre 2 (due probablement à quelque mésintelligence de la part des auditeurs de Dirichlet) est elle-même (*überflüssig*) superflue". Je me permets de répondre à M. Sylvester que sa remarque, dont je n'ai eu connaissance qu'aujourd'hui, 11 juillet 1880, repose sur un malentendu de sa part, en ce qu'il prend pour synonymes les deux mots *superflu* et *évitable*. En désignant comme superflue une opération, on veut bien dire qu'elle est aussi évitable; mais la réciproque n'est pas juste; une opération évitable peut en même temps être très-utile, et dans ce cas elle n'est pas du tout superflue. Comme M. Sylvester l'a remarqué dans une Note antérieure (*Comptes rendus*, du 3 mai 1880, p. 1054), il est évident qu'on peut toujours former une chaîne réductive impaire dont les deux premiers termes sont des nombres impairs donnés. Je me permets d'ajouter que certainement cette évidence n'a pu échapper à personne et que l'algorithme de M. Sylvester coïncide à peu près avec celui que Eisenstein a publié il y a trente-six ans (*Journal de Crelle*, t. 27, p. 317); mais, en excluant les restes pairs et en évitant ainsi la décomposition relative au nombre 2, on est amené très sou-

vent à une chaîne réductive beaucoup plus longue; sans aucun doute, l'illustre géomètre anglais se serait aperçu de cette circonstance s'il avait voulu traiter, non seulement le deuxième et le troisième, mais aussi le premier des exemples proposés à l'endroit cité de la *Zahlentheorie* (p. 110). En effet, pour calculer d'après la méthode des restes impairs la valeur du symbole $\left(\frac{365}{1847}\right)$, il faut former la chaîne réductive contenant les 21 nombres suivants:

1847, 365, — 343, — 321, 299, 277, — 255,
— 233, 211, 189, — 167, — 145, 123, 101,
— 79, — 51, 35, 13, 9, — 5, — 1,

tandis que, dans la méthode des plus petits restes, il suffit de former seulement les deux chaînes

1847, 365, 22 et 365, 11, 2.

Je suis persuadé que tout calculateur préférera la dernière méthode, et j'en conclus que la conservation des restes pairs et de la décomposition relative au nombre 2, bien qu'elle soit évitable, n'est pas du tout superflue, comme le veut M. Sylvester. Je laisse donc au lecteur le soin de juger de quel côté se trouve la mésintelligence; sans doute, j'aurais pu éviter d'entrer dans cette discussion, provoquée par M. Sylvester, mais j'espère que ma réponse ne sera pas tout à fait superflue.

XVIII.

Theorie der algebraischen Funktionen einer Veränderlichen.

[In Gemeinschaft mit Heinrich Weber veröffentlicht im Journal für reine und angewandte Mathematik, Bd. 92, S. 181—290, 1882 (datiert Oktober 1880).]

Einleitung.

Die im nachstehenden mitgeteilten Untersuchungen verfolgen den Zweck, die Theorie der algebraischen Funktionen einer Veränderlichen, welche eines der Hauptergebnisse der Riemannschen Schöpfung ist, von einem einfachen und zugleich strengen und völlig allgemeinen Gesichtspunkt aus zu begründen. Bei den bisherigen Untersuchungen über diesen Gegenstand werden in der Regel gewisse beschränkende Voraussetzungen über die Singularitäten der betrachteten Funktionen gemacht, und die sogenannten Ausnahmefälle entweder als Grenzfälle beiläufig erwähnt oder auch ganz beiseite gesetzt. Ebenso werden gewisse Grundsätze über die Stetigkeit und Entwickelbarkeit zugelassen, deren Evidenz sich auf geometrische Anschauung verschiedener Art stützt. Eine sichere Basis für die Grundvorstellungen sowie für eine allgemeine und ausnahmslose Behandlung der Theorie läßt sich gewinnen, wenn man von einer Verallgemeinerung der Theorie der rationalen Funktionen einer Veränderlichen, insbesondere des Satzes, daß jede ganze rationale Funktion einer Veränderlichen sich in lineare Faktoren zerlegen läßt, ausgeht. Diese Verallgemeinerung ist einfach und bekannt in dem ersten Falle, in welchem die von Riemann mit p bezeichnete Zahl (das Geschlecht nach Clebsch) den Wert Null hat. Für den allgemeinen Fall, welcher sich zu dem eben genannten ähnlich verhält, wie der Fall der allgemeinsten algebraischen Zahlen zu demjenigen der rationalen Zahlen, wiesen die mit bestem Erfolge in der Zahlentheorie angewandten Methoden, die

sich an Kummers Schöpfung der idealen Zahlen anschließen, und der Übertragung auf die Theorie der Funktionen fähig sind, auf den richtigen Weg *).

Versteht man, analog der Zahlentheorie, unter einem Körper algebraischer Funktionen ein System solcher Funktionen von der Beschaffenheit, daß die Anwendung der vier Spezies auf Funktionen des Systems immer zu Funktionen desselben Systems führt, so deckt sich dieser Begriff vollständig mit dem der Riemannschen Klasse algebraischer Funktionen. Unter den Funktionen eines solchen Körpers kann eine beliebige als unabhängige Veränderliche und die übrigen als von ihr abhängig betrachtet werden. Für jede dieser „Darstellungsweisen" ergibt sich ein System von Funktionen des Körpers, die als ganze Funktionen zu bezeichnen sind, deren Quotienten den ganzen Körper erschöpfen. Unter diesen ganzen Funktionen lassen sich nun wieder Gruppen von Funktionen aussondern, welchen die charakteristischen Merkmale solcher ganzen rationalen Funktionen zukommen, die einen gemeinschaftlichen Teiler haben. Ein solcher Teiler existiert zwar im allgemeinen Falle nicht, wenn man aber die bezüglichen Sätze über rationale Funktionen nicht an den Teiler selbst, sondern an das System der durch denselben teilbaren Funktionen knüpft, so gestatten sie eine vollkommene Übertragung auf die allgemeinen algebraischen Funktionen. Auf diese Weise gelangt man zu dem Begriff des Ideals, ein Name, der aus Kummers zahlentheoretischen Arbeiten stammt, wo die nicht existierenden Teiler als „ideale Teiler" in die Rechnung eingeführt werden.

Obwohl es sich in der vorliegenden Arbeit keineswegs um „ideale" Funktionen handelt, sondern alle Operationen nur an Systemen wirklich existierender Funktionen ausgeführt werden, schien es doch zweck-

---

*) Die idealen Zahlen sind von Kummer zuerst eingeführt durch die Abhandlung: Zur Theorie der komplexen Zahlen (Crelles Journal, Bd. 35); eine weitere Fortführung und eine allgemeine Darstellung der Theorie der algebraischen Zahlen findet man in der zweiten und dritten Auflage von Dirichlets Vorlesungen über Zahlentheorie, sowie in der Abhandlung von Dedekind: Sur la théorie des nombres entiers algébriques (Paris 1877. Abdruck aus dem Bulletin des Sciences math. et astron. von Darboux und Houël). Die Kenntnis dieser Schriften wird aber in unserer Arbeit nirgends vorausgesetzt.

Aus mündlichen Mitteilungen ist uns jetzt bekannt geworden, daß bereits vor Jahren Kronecker mit Beziehung auf die Arbeiten von Weierstraß Untersuchungen angestellt hat, die auf derselben Grundlage, wie die unsrigen, beruhen.

mäßig, den Namen „Ideal", der in der Zahlentheorie bereits gebräuchlich ist, beizubehalten.

Mit diesen Idealen läßt sich nach gehöriger Erklärung der Multiplikation ganz nach denselben Regeln rechnen, wie mit rationalen Funktionen. Insbesondere ergibt sich der Satz, daß jedes Ideal auf eine einzige Weise in Faktoren zerlegbar ist, welche selbst nicht weiter zerlegt werden können und daher Primideale genannt werden. Diese Primideale entsprechen den linearen Faktoren in der Theorie der ganzen rationalen Funktionen. Auf Grund derselben gelangt man zu einer völlig präzisen und allgemeinen Definition des „Punktes der Riemannschen Fläche", d. h. eines vollkommen bestimmten Systems von Zahlwerten, welche man den Funktionen des Körpers widerspruchslos beilegen kann.

Eine darauf gegründete formale Definition des Differentialquotienten führt sodann zu der Geschlechtszahl und zu einer ganz allgemeinen, eleganten Darstellung der Differentiale erster Gattung. Hieran schließt sich der Beweis des Riemann-Rochschen Satzes über die Anzahl der willkürlichen Konstanten in einer durch ihre Unendlichkeitspunkte bestimmten Funktion, und die Theorie der Differentiale zweiter und dritter Gattung. Bis zu diesem Punkte kommt die Stetigkeit und Entwickelbarkeit der untersuchten Funktionen in keiner Weise in Betracht. Es würde z. B. nirgends eine Lücke bleiben, wenn man das Gebiet der benutzten Zahlen auf das System der algebraischen Zahlen beschränken wollte. Dadurch wird ein wohl abgegrenzter und ziemlich umfassender Teil der Theorie der algebraischen Funktionen lediglich durch die seiner eigenen Sphäre angehörigen Mittel behandelt.

Freilich ergeben sich alle diese Resultate durch einen weit geringeren Aufwand von Mitteln und als Spezialfälle einer vielumfassenden Allgemeinheit aus Riemanns Theorie; allein es ist bekannt, daß diese Theorie bezüglich einer strengen Begründung noch gewisse Schwierigkeiten bietet, und bis es gelungen ist, diese Schwierigkeiten vollständig zu überwinden, dürfte der von uns betretene Weg oder wenigstens ein verwandter, wohl der einzige sein, der für die Thorie der algebraischen Funktionen mit befriedigender Strenge und Allgemeinheit zum Ziele führt. So würde sich die Theorie der Ideale selbst außerordentlich vereinfachen, wenn man den Begriff der Riemannschen Fläche und insbesondere den eines

Punktes derselben samt den auf die Stetigkeit der algebraischen Funktionen gegründeten Anschauungen voraussetzen wollte. In unserer Arbeit ist umgekehrt auf einem langen Umwege die Theorie der Ideale algebraisch begründet und aus dieser eine vollkommen präzise und strenge Definition des „Punktes der Riemannschen Fläche“ gewonnen, welche auch als Basis für die Untersuchung der Stetigkeit und der damit zusammenhängenden Fragen dienen kann. Diese Fragen, wozu auch die auf die Abelschen Integrale und die Periodizitätsmoduln bezüglichen gehören, bleiben von unserer Untersuchung einstweilen ausgeschlossen. Wir hoffen bei einer anderen Gelegenheit darauf zurückzukommen.

Königsberg, den 22. Oktober 1880.

I. Abteilung.

§ 1.

Körper algebraischer Funktionen.

Eine Variable θ heißt eine algebraische Funktion einer unabhängigen Veränderlichen z, wenn dieselbe einer irreduktibeln algebraischen Gleichung

(1) $$F(\theta, z) = 0$$

genügt. F bedeutet hierin einen Ausdruck von der Form

$$F(\theta, z) = a_0 \theta^n + a_1 \theta^{n-1} + \cdots + a_{n-1}\theta + a_n,$$

worin die Koeffizienten $a_0, a_1, \cdots a_n$ ganze rationale Funktionen von z ohne gemeinschaftlichen Teiler sind. Die vorausgesetzte Irreduktibilität der Gleichung (1) involviert, daß θ nicht einer Gleichung niedrigeren Grades in bezug auf θ genügt, und, wie sich aus dem Algorithmus des größten gemeinschaflichen Teilers ergibt, wenn

$$G(\theta, z) = b_0 \theta^m + b_1 \theta^{m-1} + \cdots + b_{m-1}\theta + b_m = 0$$

eine zweite Gleichung ist, welcher θ genügt, daß $G(\theta, z)$ durch $F(\theta, z)$ algebraisch teilbar sein muß. Es läßt sich nun nachweisen, daß $G(\theta, z)$ auch in bezug auf z nicht von niedrigerem Grade sein kann als $F(\theta, z)$ und nur dann vom selben Grade, wenn sich aus $G(\theta, z)$ ein von z unabhängiger Faktor absondern läßt. Nehmen wir an, die Koeffizienten $b_0, b_1, \cdots b_m$ seien von gemeinschaftlichen Faktoren befreit, und bezeichnen wir mit

$$H(\theta, z) = c_0 \theta^{m-n} + c_1 \theta^{m-n-1} + \cdots + c_{m-n}$$

den vom Nenner befreiten Quotienten von G durch F, so ist

$$kG(\theta, z) = F(\theta, z) \cdot H(\theta, z),$$

worin k eine ganze rationale Funktion von z ist, und die Vergleichung der Koeffizienten ergibt

$$\begin{aligned} k b_0 &= a_0 c_0, \\ k b_1 &= a_0 c_1 + a_1 c_0, \\ k b_2 &= a_0 c_2 + a_1 c_1 + a_2 c_0, \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

worin die $c_0, c_1, \cdots c_{m-n}$ gleichfalls ohne gemeinschaftlichen Teiler vorausgesetzt werden können.

Hieraus folgt zunächst, daß k konstant sein muß, und $= 1$ gesetzt werden kann; denn ist durch irgend einen Linearfaktor von $k\, a_0, a_1, \cdots a_{r-1}, c_0, c_1, \cdots c_{s-1}$ teilbar, a_r, c_s nicht teilbar, so folgt aus

$$k b_{r+s} = \cdots a_{r-1} c_{s+1} + a_r c_s + a_{r+1} c_{s-1} + \cdots$$

der Widerspruch, daß $a_r c_s$ durch denselben Linearfaktor teilbar sein müßte. Hieraus aber folgt weiter, daß der Grad von $G(\theta, z)$ in bezug auf z gleich ist der Summe der Grade von F und H in bezug auf z; denn sind a_r, c_s die ersten unter den Koeffizienten a, c, deren Grad den Maximalwert erreicht, so folgt wieder aus

$$b_{r+s} = \cdots a_{r-1} c_{s+1} + a_r c_s + a_{r+1} c_{-1} + \cdots,$$

daß der Grad von b_{r+s} gleich der Summe der Grade von a_r und c_s ist.

Dividiert man die Gleichung (1) durch a_0, so kann dieselbe auch in die Form gesetzt werden

$$(2) \qquad f(\theta, z) = \theta^n + b_1 \theta^{n-1} + \cdots + b_{n-1}\theta + b_n = 0,$$

worin die Koeffizienten $b_1, b_2, \cdots b_n$ auch gebrochene rationale Funktionen von z sein können.

Das System aller rationalen Funktionen von θ und z, $\Phi(\theta, z)$, hat die Eigenschaft, daß seine Individuen sich durch die elementaren Rechenoperationen, Addition, Subtraktion, Multiplikation und Division reproduzieren, und dies System wird daher als ein Körper algebraischer Funktionen Ω vom Grade n bezeichnet. Ist zunächst $\varphi(\theta)$ eine ganze rationale Funktion von θ, deren Koeffizienten rational von z abhängen, so kann man durch algebraische Division zwei eben solche Funktionen $q(\theta)$, $r(\theta)$ bestimmen, von denen die zweite den Grad $n-1$ nicht übersteigt, so daß

$$\varphi(\theta) = q(\theta) f(\theta) + r(\theta)$$

oder wegen (2)

$$\varphi(\theta) = r(\theta).$$

Ist $\varphi(\theta)$ durch $f(\theta)$ nicht teilbar, so haben diese beiden Funktionen [wegen der vorausgesetzten Irreduktibilität von $f(\theta)$] keinen Teiler gemein, und daher lassen sich durch die Methode des größten gemeinschaftlichen Teilers zwei Funktionen $f_1(\theta), \varphi_1(\theta)$ so bestimmen, daß

$$f(\theta) f_1(\theta) + \varphi(\theta) \varphi_1(\theta) = 1,$$

also wegen (2)

$$\varphi_1(\theta) = \frac{1}{\varphi(\theta)}.$$

Aus diesen beiden Bemerkungen, zusammengenommen mit der Voraussetzung der Irreduktibilität von $f(\theta)$ ergibt sich der folgende

Lehrsatz. Jede Funktion ζ des Körpers Ω läßt sich auf eine einzige Weise in die Form setzen:

$$\zeta = x_0 + x_1 \theta + \cdots + x_{n-1} \theta^{n-1},$$

worin die Koeffizienten $x_0, x_1, \cdots x_{n-1}$ rationale Funktionen von z sind. Umgekehrt gehört jede Funktion dieser Form selbstverständlich dem Körper Ω an.

Wählt man unter den Funktionen des Körpers Ω n beliebige aus:

$$\begin{aligned}
\eta_1 &= x_0^{(1)} + x_1^{(1)} \theta + \cdots + x_{n-1}^{(1)} \theta^{n-1}, \\
\eta_2 &= x_0^{(2)} + x_1^{(2)} \theta + \cdots + x_{n-1}^{(2)} \theta^{n-1}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\eta_n &= a_0^{(n)} + x_1^{(n)} \theta + \cdots + x_{n-1}^{(n)} \theta^{n-1},
\end{aligned}$$

jedoch so, daß die Determinante

$$\sum \pm x_0^{(1)} x_1^{(2)} \cdots x_{n-1}^{(n)}$$

nicht identisch Null ist, so ergibt sich, daß jede Funktion des Körpers Ω auch in der Form dargestellt werden kann

$$\zeta = y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n,$$

deren Koeffizienten $y_1, y_2, \cdots y_n$ rationale Funktionen von z sind. Ein solches System von Funktionen $\eta_1, \eta_2, \cdots \eta_n$ soll eine Basis des Körpers Ω heißen.

Damit ein Funktionensystem $\eta_1, \eta_2, \cdots \eta_n$ des Körpers Ω eine Basis desselben bilde, ist erforderlich und hinreichend, daß zwischen ihnen keine Gleichung (Identität) von der Form

$$y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n = 0$$

bestehe, in welcher die Koeffizienten $y_1, y_2, \cdots y_n$ nicht sämtlich verschwinden. Beispielsweise bilden die Funktionen $1, \theta, \theta^2, \cdots \theta^{n-1}$ eine Basis von Ω.

§ 2.

Normen, Spuren und Diskriminanten.

Wählt man zur Darstellung der Funktionen von Ω eine beliebige Basis $\eta_1, \eta_2, \cdots \eta_n$, so kann man, wenn ζ irgend eine Funktion in Ω bedeutet, setzen:

$$(1)\qquad \begin{cases} \zeta\eta_1 = y_{1,1}\eta_1 + y_{1,2}\eta_2 + \cdots + y_{1,n}\eta_n, \\ \zeta\eta_2 = y_{2,1}\eta_1 + y_{2,2}\eta_2 + \cdots + y_{2,n}\eta_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \zeta\eta_n = y_{n,1}\eta_1 + y_{n,2}\eta_2 + \cdots + y_{n,n}\eta_n, \end{cases}$$

worin die Koeffizienten $y_{\iota,\iota'}$ rationale Funktionen von z sind. Hieraus ergibt sich die Gleichung

$$(2)\qquad \begin{vmatrix} y_{1,1}-\zeta, & y_{1,2}, & \cdots & y_{1,n} \\ y_{2,1}, & y_{2,2}-\zeta, & \cdots & y_{2,n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ y_{n,1}, & y_{n,2}, & \cdots & y_{n,n}-\zeta \end{vmatrix} = 0,$$

welche, nach Potenzen von ζ geordnet, die Gestalt hat

$$(3)\qquad \varphi(\zeta) = \zeta^n + b_1\zeta^{n-1} + \cdots + b_{n-1}\zeta + b_n = 0$$

und, wie sich aus dem Multiplikationssatz der Determinanten ohne Schwierigkeit ergibt, von der Wahl der zugrunde gelegten Basis $\eta_1, \eta_2, \cdots \eta_n$ ganz unabhängig ist. Von den Koeffizienten $b_1, b_2, \cdots b_n$ der Funktion φ, welche sämtlich rationale Funktionen von z und durch die Funktion ζ vollkommen bestimmt sind, sollen zwei, die in der Folge von Wichtigkeit sind, durch besondere Namen ausgezeichnet werden. Die Funktion

$$(4)\qquad (-1)^n b_n = \begin{vmatrix} y_{1,1}, & y_{1,2}, & \cdots & y_{1,n} \\ y_{2,1}, & y_{2,2}, & \cdots & y_{2,n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ y_{n,1}, & y_{n,2}, & \cdots & y_{n,n} \end{vmatrix}$$

heißt die Norm der Funktion ζ, und wird mit $N(\zeta)$ bezeichnet Von dieser Funktion gelten folgende Sätze.

1. Die einzige Funktion, deren Norm identisch verschwindet, ist die Funktion „Null“; denn macht man in dem System (1) die Annahme daß $N(\zeta) = 0$ sei, so folgt, daß sich ein System rationaler Funktionen von z, die nicht sämtlich verschwinden, $y_1, y_2, \cdots y_n$ so bestimmen läßt, daß

$$\zeta(y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n) = 0,$$

also, da $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden, $\zeta = 0$.

2. Die Norm einer rationalen Funktion von z ist die n^{te} Potenz dieser Funktion. Denn ist ζ rational, so reduzieren sich die Gleichungen (1) auf die Identitäten $\zeta\,\eta_h = \zeta\,\eta_h$, woraus $N(\zeta) = \zeta^n$ folgt.

3. Ist ζ' irgend eine zweite Funktion des Körpers Ω und das dem System (1) entsprechende Gleichungssystem für diese Funktion

$$\zeta'\,\eta_h = \sum_{i} y'_{h,i}\,\eta_i,$$

so folgt:

$$\zeta\,\zeta'\,\eta_h = \sum_{i,i'} y_{h,i}\,y'_{i,i'}\,\eta_{i'}$$

und daraus nach dem Multiplikationssatz der Determinanten

$$N(\zeta\zeta') = N(\zeta)\,N(\zeta').$$

4. Aus 2. und 3. folgt:

$$N(\zeta)\,N\left(\frac{1}{\zeta}\right) = 1,$$

also:

$$N\left(\frac{\zeta}{\zeta'}\right) = \frac{N(\zeta)}{N(\zeta')}.$$

5. Endlich ergibt sich aus der Definition der Funktion φ, (2), (3) der wichtige Satz: Ist t eine beliebige Konstante (oder auch eine rationale Funktion von z), so ist

$$\varphi(t) = N(t-\zeta).$$

Es soll sodann die Funktion

$$-b_1 = y_{1,1} + y_{2,2} + \cdots + y_{n,n} \tag{5}$$

die Spur von ζ genannt und mit $S(\zeta)$ bezeichnet werden. Für diese ergeben sich unmittelbar aus der Definition die Sätze:

$$S(0) = 0, \tag{6}$$

$$S(1) = n. \tag{7}$$

Und wenn x eine rationale Funktion von z, ferner ζ, ζ' zwei Funktionen in Ω bedeuten:

$$S(x\zeta) = x\,S(\zeta), \tag{8}$$

$$S(\zeta+\zeta') = S(\zeta) + S(\zeta'). \tag{9}$$

Es hat sich aus dieser Betrachtung ergeben, daß jede Funktion ζ in Ω einer Gleichung n^{ten} Grades, $\varphi(\zeta) = 0$, genügt, deren Koeffizienten rational von z abhängen. Wenn diese Gleichung irreduktibel ist, so bilden die Funktionen $1, \zeta, \zeta^2, \cdots \zeta^{n-1}$ eine Basis von Ω. Im andern Falle sei

$$\varphi_1(\zeta) = \zeta^e + b'_0\zeta^{e-1} + \cdots + b'_{e-1}\zeta + b'_e = 0 \tag{10}$$

die Gleichung niedrigsten Grades, deren Koeffizienten in z rational sind, welcher die Funktion ζ genügt, und mithin $\varphi_1(\zeta) = 0$ irreduktibel, $e < n$. Da gleichwohl $\varphi(\zeta)$ verschwindet, so muß $\varphi(\zeta)$ durch $\varphi_1(\zeta)$ algebraisch teilbar sein, und wie in § 1 ergibt sich, daß jede rationale Funktion η von z und ζ in der Form darstellbar ist

$$\eta = x_0 + x_1\zeta + \cdots + x_{e-1}\zeta^{e-1},$$

deren Koeffizienten $x_0, x_1, \cdots x_{e-1}$ rational von z abhängen *). Ist nun

$$\theta^f + \eta_1\theta^{f-1} + \cdots + \eta_{f-1}\theta + \eta_f = 0$$

die Gleichung niedrigsten Grades, welcher θ genügt, deren Koeffizienten rational von z und ζ abhängen, so besteht zwischen den $e.f$ Funktionen

$$\zeta^h\theta^k \qquad (h = 0, 1, \cdots e-1;\ k = 0, 1, \cdots f-1) \tag{11}$$

keine lineare Gleichung mit rational von z abhängigen Koeffizienten, während jede Funktion in Ω linear mit rational von z abhängigen Koeffizienten durch diese Funktionen darstellbar ist. Es ergibt sich daraus, daß dieselben eine Basis von Ω bilden, und daß sonach

$$e.f = n,$$

also e ein Teiler von n ist.

Wendet man die Basis (11) zur Aufstellung der Norm von ζ an, so erkennt man leicht mittels der Gleichung (10), daß

$$N(\zeta) = ((-1)^e b'_e)^f = (-1)^n b'^f_e$$

wird. Da ferner für ein beliebiges konstantes t die Funktion $\zeta - t$ einer Gleichung von demselben Grade genügt wie ζ, so ergibt sich der Satz:

Die Funktion $\varphi(t)$ (3) ist entweder irreduktibel oder eine ganze Potenz einer irreduktibeln Funktion.

Ist $\eta_1, \eta_2, \cdots \eta_n$ ein beliebiges System von n Funktionen in Ω, gleichviel ob dasselbe eine Basis bildet oder nicht, so führen wir eine zu diesem System gehörige rationale Funktion von z ein, die wir als dessen Diskriminante, $\Delta(\eta_1, \eta_2, \cdots \eta_n)$ bezeichnen und folgendermaßen definieren

$$\Delta(\eta_1, \eta_2, \cdots \eta_n) = \begin{vmatrix} S(\eta_1\eta_1), & S(\eta_1\eta_2), & \cdots & S(\eta_1\eta_n) \\ S(\eta_2\eta_1), & S(\eta_2\eta_2), & \cdots & S(\eta_2\eta_n) \\ \cdots & \cdots & \cdots & \cdots \\ S(\eta_n\eta_1), & S(\eta_n\eta_2), & \cdots & S(\eta_n\eta_n) \end{vmatrix}. \tag{12}$$

*) Aus der Gleichung $\varphi_1(\zeta) = 0$ entspringt ein Körper algebraischer Funktionen Ω_1 vom Grade e, dessen Funktionen sämtlich zugleich im Körper Ω enthalten sind, und der daher als ein Teiler des Körpers Ω bezeichnet werden kann.

Die Diskriminante ist dann und nur dann nicht identisch Null, wenn die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden.

Um den ersten Teil dieser Behauptung zu beweisen, nehmen wir an, es sei $\Delta(\eta_1, \eta_2, \cdots \eta_n) = 0$. Es läßt sich unter dieser Voraussetzung ein System rationaler Funktionen $y_1, y_2, \cdots y_n$ von z, die nicht alle identisch verschwinden, so bestimmen, daß

$$\begin{aligned} &y_1 S(\eta_1 \eta_k) + y_2 S(\eta_2 \eta_k) + \cdots + y_n S(\eta_n \eta_k) \\ &= S\Big(\eta_k \underset{(k = 1, 2, \cdots n)}{(y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n)}\Big) = 0. \end{aligned}$$

Wählt man daher ein System rationaler Funktionen $x_1, x_2, \cdots x_n$ von z, ganz beliebig und setzt:

$$\begin{aligned} y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n &= \eta, \\ x_1 \eta_1 + x_2 \eta_2 + \cdots + x_n \eta_n &= \zeta, \end{aligned}$$

so folgt:

$$S(\zeta \eta) = 0.$$

Wenn aber die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden, so kann ζ jede beliebige Funktion in Ω, also, da η nicht verschwindet, beispielsweise auch $\frac{1}{\eta}$ sein. Dann ist aber die letzte Gleichung sicher nicht erfüllt, und es kann also unter dieser Voraussetzung die Diskriminante von $\eta_1, \eta_2, \cdots \eta_n$ nicht identisch verschwinden.

Halten wir die Annahme fest, daß $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω sei, und setzen:

$$\eta'_k = x_{1,k} \eta_1 + x_{2,k} \eta_2 + \cdots + x_{n,k} \eta_n, \qquad (k = 1, 2, \cdots n)$$

so bilden die Funktionen $\eta'_1, \eta'_2, \cdots \eta'_n$ eine Basis von Ω oder nicht, je nachdem die Determinante der rationalen Funktionen $x_{h,k}$ von z

$$X = \sum \pm x_{1,1} x_{2,2} \cdots x_{n,n}$$

von Null verschieden ist oder nicht. Nun ist aber

$$S(\eta'_h \eta'_k) = \sum_{1, n}^{i, i'} x_{i,h} x_{i',k} S(\eta_i \eta_{i'}),$$

und daraus ergibt sich nach dem Multiplikationssatz der Determinanten der **Hauptsatz über die Diskriminanten**

$$\Delta(\eta'_1, \eta'_2, \cdots \eta'_n) = X^2 \Delta(\eta_1, \eta_2, \cdots \eta_n), \tag{13}$$

woraus auch die Richtigkeit des zweiten Teils der obigen Behauptung erhellt, daß die Diskriminante eines Funktionensystems stets dann identisch verschwindet, wenn dasselbe keine Basis von Ω bildet.

§ 3.

Das System der ganzen Funktionen von z im Körper Ω.

Definition. Eine Funktion ω des Körpers Ω soll eine ganze Funktion von z heißen, wenn in der Gleichung niedrigsten Grades, welcher dieselbe nach § 2 genügt:

$$(1) \qquad \varphi(\omega) = \omega^e + b_1\omega^{e-1} + \cdots + b_{e-1}\omega + b_e = 0,$$

die Koeffizienten $b_1, b_2, \cdots b_e$ ganze rationale Funktionen von z sind; im entgegengesetzten Fall heiße sie eine gebrochene Funktion. Der Inbegriff aller ganzen Funktionen von z in Ω soll mit $\mathfrak{o}$ bezeichnet werden. Da nach § 2 $N(t-\omega)$ eine ganze Potenz von $\varphi(t)$ ist, so folgt, daß für eine ganze Funktion ω auch die sämtlichen Koeffizienten von $N(t-\omega)$ ganze rationale Funktionen von z sind, also insbesondere:

1. Die Norm und die Spur einer ganzen Funktion sind ganze rationale Funktionen von z.

Aus der Definition der ganzen Funktionen ergibt sich ferner:

2. Eine rationale Funktion von z gehört dann und nur dann zu dem System $\mathfrak{o}$, wenn sie eine ganze rationale Funktion von z ist.

3. Jede Funktion η in Ω kann durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Funktion von z in eine Funktion des Systems $\mathfrak{o}$ verwandelt werden. Denn es genügt η nach § 2 einer Gleichung niedrigsten Grades von der Form

$$b_0\eta^e + b_1\eta^{e-1} + \cdots + b_{e-1}\eta + b_e = 0,$$

deren Koeffizienten ganze rationale Funktionen von z sind, und diese geht durch die Substitution $b_0\eta = \omega$ in eine Gleichung von der Form (1) für ω über.

4. Eine Funktion ω des Körpers Ω, welche irgend einer Gleichung von der Form genügt

$$\psi(\omega) = \omega^m + c_1\omega^{m-1} + \cdots + c_{m-1}\omega + c_m = 0,$$

in welcher die Koeffizienten $c_1, \cdots c_m$ ganze rationale Funktionen von z sind, ist eine ganze Funktion. Denn ist

$$\varphi(\omega) = \omega^e + b_1\omega^{e-1} + \cdots + b_{e-1}\omega + b_e = 0$$

die Gleichung niedrigsten Grades, welcher ω genügt, so muß $\psi(\omega)$ durch $\varphi(\omega)$ algebraisch teilbar sein:

$$\psi(\omega) = \varphi(\omega)\chi(\omega),$$

was, wie leicht zu zeigen ist, zur Folge hat, daß auch die Koeffizienten von $\varphi(\omega)$ und $\chi(\omega)$ ganze rationale Funktionen von z sind (Gauß,

Disq. Ar. art. 42). Hieraus ergibt sich der Hauptsatz über die ganzen Funktionen:

5. Summe, Differenz, Produkt zweier ganzen Funktionen sind wieder ganze Funktionen.

Sind nämlich ω', ω'' zwei ganze Funktionen in $\mathfrak{Q}$, welche resp. den Gleichungen genügen

$$\omega'^{n'} + b'_1 \omega'^{n'-1} + \cdots + b'_{n'-1}\, \omega' + b'_{n'} = 0,$$
$$\omega''^{n''} + b''_1 \omega''^{n''-1} + \cdots + b''_{n''-1} \omega'' + b''_{n''} = 0,$$

so kann man, wenn man unter $\omega_1, \omega_2, \cdots \omega_m$ die $m = n' n''$ Produkte

$$\omega'^{h'} \omega''^{h''} \quad (h' = 0, 1, \cdots n'-1;\ h'' = 0, 1, \cdots n''-1)$$

und unter ω eine der drei Funktionen $\omega' \pm \omega''$, $\omega' \omega''$ versteht, setzen

$$\omega\, \omega_1 = x_{1,1}\, \omega_1 + \cdots + x_{1,m}\, \omega_m,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\omega\, \omega_m = x_{m,1}\, \omega_1 + \cdots + x_{m,m}\, \omega_m,$$

worin die $x_{h,h'}$ ganze rationale Funktionen von z sind, und daraus erhält man

$$\begin{vmatrix} x_{1,1} - \omega, & x_{1,2}, & \cdots x_{1,m} \\ x_{2,1}, & x_{2,2} - \omega, & \cdots x_{2,m} \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \\ x_{m,1}, & x_{m,2}, & \cdots x_{m,m} - \omega \end{vmatrix} = 0,$$

also eine Gleichung für ω, deren Koeffizienten ganze rationale Funktionen von z sind.

Als Korollar ergibt sich hieraus, daß jede ganze rationale Funktion von Funktionen in $\mathfrak{o}$ selbst eine Funktion des Systems $\mathfrak{o}$ ist.

6. Eine ganze Funktion ω heißt durch eine andere ganze Funktion ω' teilbar, wenn ein dritte ganze Funktion ω'' existiert, welche der Bedingung genügt

$$\omega = \omega' \omega''.$$

Aus dieser Definition ergibt sich sofort:

Ist ω teilbar durch ω', ω' durch ω'', so ist auch ω durch ω'' teilbar.

Ist ω' und ω'' durch ω teilbar, so ist auch $\omega' \pm \omega''$ durch ω teilbar, und allgemein: sind $\omega_1, \omega_2, \omega_3, \cdots$ durch ω teilbar, $\omega'_1, \omega'_2, \omega'_3, \cdots$ beliebige Funktionen in $\mathfrak{o}$, so ist auch $\omega'_1 \omega_1 + \omega'_2 \omega_2 + \omega'_3 \omega_3 + \cdots$ durch ω teilbar.

7. Bilden die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω, so kann man (nach 3.) n von Null verschiedene ganze rationale Funktionen von z, $a_1, a_2, \cdots a_n$ der Art bestimmen, daß

$$\omega_1 = a_1 \eta_1, \ \omega_2 = a_2 \eta_2, \cdots \omega_n = a_n \eta_n$$

ganze Funktionen sind, und diese bilden ebenfalls eine Basis von Ω, da

$$\Delta(\omega_1, \omega_2, \cdots \omega_n) = a_1^2 a_2^2 \cdots a_n^2 \Delta(\eta_1, \eta_2, \eta_n)$$

von Null verschieden ist. Es gibt also Basen von Ω, $\omega_1, \omega_2, \cdots \omega_n$, welche aus lauter ganzen Funktionen bestehen, und die Diskriminante einer solchen Basis ist, da $S(\omega_r \omega_s)$ ganze rationale Funktionen von z sind, selbst eine von Null verschiedene ganze rationale Funktion von z. Jede Funktion von der Form

$$\omega = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n, \tag{2}$$

in welcher die $x_1, x_2, \cdots x_n$ ganze rationale Funktionen von z sind, gehört dann zu dem System $\mathfrak{o}$; aber es ist durchaus nicht notwendig, daß umgekehrt jede Funktion in $\mathfrak{o}$ in dieser Form darstellbar sei.

Nehmen wir also an, es existieren in $\mathfrak{o}$ noch andere Funktionen als die in der Form (2) enthaltenen, so müssen sich eine lineare Funktion $z - c$ und gewisse ganze rationale Funktionen $x_1, x_2, \cdots x_n$, die nicht alle durch $z - c$ teilbar sind, so wählen lassen, daß

$$\frac{x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n}{z - c}$$

eine ganze Funktion ist. Die Funktionen $x_1, x_2, \cdots x_n$ lassen sich nun auf ihre nicht sämtlich verschwindenden konstanten Reste $c_1, c_2, \cdots c_n$ in bezug auf $z - c$ reduzieren, und daraus erhellt, daß auch

$$\omega = \frac{c_1 \omega_1 + c_2 \omega_2 + \cdots + c_n \omega_n}{z - c}$$

eine ganze Funktion ist. Ist c_1 von Null verschieden, so bilden auch die n ganzen Funktionen

$$\omega \text{ und } \omega_2, \omega_3, \cdots \omega_n$$

eine Basis von Ω und zugleich ist nach § 2 (13)

$$\Delta(\omega, \omega_2, \cdots \omega_n) = \frac{c_1^2}{(z-c)^2} \Delta(\omega_1, \omega_2, \cdots \omega_n),$$

also von niedrigerem Grade als $\Delta(\omega_1, \omega_2, \cdots \omega_n)$. Da nun diese beiden Diskriminanten ganze rationale Funktionen von z sind, so gelangt man durch wiederholte Anwendung dieses Verfahrens schließlich zu einer aus ganzen Funktionen bestehenden Basis von Ω, $\omega_1', \omega_2', \cdots \omega_n'$, deren Diskriminante im Grade nicht weiter erniedrigt werden kann,

und welche folglich die Eigenschaft hat, daß **jede** Funktion ω in $\mathfrak{o}$ in der Form enthalten ist

$$\omega = x_1 \omega_1' + x_2 \omega_2' + \cdots + x_n \omega_n'$$

mit ganzen rationalen Funktionen von z als Koeffizienten. Ein solches System soll eine Basis von $\mathfrak{o}$ genannt werden.

Ist $\omega_1, \omega_2, \cdots \omega_n$ eine Basis von $\mathfrak{o}$ und

$$\omega_\iota' = x_{\iota,1}\omega_1 + x_{\iota,2}\omega_2 + \cdots + x_{\iota,n}\omega_n, \qquad (\iota = 1, 2, \cdots n)$$

so wird das System $\omega_1', \omega_2', \cdots \omega_n'$ dann und nur dann ebenfalls eine Basis von $\mathfrak{o}$ bilden, wenn die Determinante der ganzen rationalen Funktionen $x_{\iota,\iota'}$

$$X = \sum \pm x_{1,1}\, x_{2,2} \cdots x_{n,n}$$

eine von Null verschiedene Konstante ist. Denn nehmen wir an, es habe diese Determinante irgend einen Linearfaktor $z - c$, so lassen sich Konstanten $c_1, c_2, \cdots c_n$, nicht sämtlich verschwindend, so bestimmen, daß die n ganzen rationalen Funktionen von z

$$c_1 x_{1,\iota} + c_2 x_{2,\iota} + \cdots + c_n x_{n,\iota}$$

durch $z - c$ teilbar werden (d. h. für $z = c$ verschwinden); dann aber ist

$$\frac{c_1 \omega_1' + c_2 \omega_2' + \cdots + c_n \omega_n'}{z - c}$$

eine ganze Funktion und mithin $\omega_1', \omega_2', \cdots \omega_n'$ keine Basis von $\mathfrak{o}$.

Da nun andererseits

$$\Delta(\omega_1', \omega_2' \cdots \omega_n') = X^2 \Delta(\omega_1, \omega_2, \cdots \omega_n)$$

ist, so folgt, daß die Diskriminante einer Basis von $\mathfrak{o}$ von einem konstanten Faktor abgesehen von der Wahl dieser Basis unabhängig ist. Man erhält also eine vollkommen bestimmte ganze rationale Funktion von z, wenn man in der Diskriminante einer beliebigen Basis von $\mathfrak{o}$ den Koeffizienten der höchsten Potenz von z durch Division $= 1$ macht. Diese Funktion soll die Diskriminante des Körpers Ω oder des Systems $\mathfrak{o}$ genannt und mit $\Delta(\Omega)$ oder $\Delta(\mathfrak{o})$ bezeichnet werden.

§ 4.

Die Funktionenmoduln.

Wir betrachten im folgenden Systeme von Funktionen, welche wir Funktionenmoduln oder auch schlechtweg Moduln nennen und folgendermaßen definieren. Ein Funktionensystem (in Ω) heißt

ein Modul, wenn sich die Funktionen desselben durch Addition, Subtraktion und durch Multiplikation mit ganzen rationalen Funktionen von z reproduzieren.

Bezeichnet man mit $\alpha_1, \alpha_2, \cdots \alpha_m$ irgend m gegebene Funktionen, mit $x_1, x_2, \cdots x_m$ willkürliche ganze rationale Funktionen von z, so bildet der Inbegriff aller Funktionen von der Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m$$

einen Modul. Ein solcher soll ein endlicher Modul genannt und mit

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_m]$$

bezeichnet werden. Das Funktionensystem $\alpha_1, \alpha_2, \ldots \alpha_m$ heißt die Basis dieses Moduls.

Wir wollen ein Funktionensystem $\alpha_1, \alpha_2, \cdots \alpha_m$ rational irreduktibel oder die Funktionen $\alpha_1, \alpha_2, \cdots \alpha_m$ rational unabhängig nennen, wenn eine Gleichung von der Form

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m = 0$$

für rationale x nur dann bestehen kann, wenn $x_1 = 0, x_2 = 0, \cdots x_m = 0$ ist. Ein Funktionensystem, welches eine Basis des Körpers Ω bildet, ist daher stets rational irreduktibel, und es gibt kein System von mehr als n rational unabhängigen Funktionen in Ω.

Wir beweisen nun zunächst den Satz:

1. Jeder endliche Modul besitzt eine rational irreduktible Basis.

Der Beweis desselben ergibt sich unmittelbar aus dem folgenden Hilfssatz:

Sind die ganzen rationalen Funktionen $y_{1,1}, y_{2,1}, \cdots y_{m,1}$ ohne gemeinschaftlichen Teiler, so lassen sich andere ganze rationale Funktionen $y_{1,2}, y_{2,2}, \cdots y_{m,m}$ so bestimmen, daß

$$\sum \pm y_{1,1}\, y_{2,2} \cdots y_{m,m} = 1 \text{ *).}$$

*) Der Satz ist richtig und bekannt für $m = 2$. Nehmen wir also an, er sei bewiesen für $m - 1$, so können wir, wenn ∂ den größten gemeinschaftlichen Teiler von $y_{1,1}, y_{2,1}, \cdots y_{m-1,1}$ bedeutet, der Gleichung genügen

$$\begin{vmatrix} y_{1,1}, & y_{2,1}, & \cdots y_{m-1,1} \\ y_{1,2}, & y_{2,2}, & \cdots y_{m-1,2} \\ \cdots & \cdots & \cdots \\ y_{1,m}, & y_{2,m} & \cdots y_{m-1,m} \end{vmatrix} = \partial$$

und wenn wir also die ganzen rationalen Funktionen x, y so bestimmen, daß

$$x\, y_{m,1} - y\,\partial = (-1)^{m-1}$$

Genügen nun die Funktionen $\alpha_1, \alpha_2, \cdots \alpha_m$ einer Gleichung

$$\sum_{1,\,m}^{\iota} y_{\iota,1}\, \alpha_\iota = 0,$$

in welcher die ganzen rationalen Funktionen $y_{1,1} \cdots y_{m,1}$ ohne gemeinschaftlichen Teiler angenommen werden können, so setze man

$$\sum_{1,\,m}^{\iota} y_{\iota,2}\, \alpha_\iota = \beta_2,$$

$$\cdots\cdots\cdots$$

$$\sum_{1,\,m}^{\iota} y_{\iota,m}\, \alpha_\iota = \beta_m;$$

dann ist der Modul $[\alpha_1, \alpha_2, \alpha_m]$ völlig identisch mit dem Modul $[\beta_2, \beta_3, \beta_m]$, dessen Basis eine Funktion weniger enthält. Sind die Funktionen β_ι noch nicht rational unabhängig, so kann man sie in derselben Weise weiter reduzieren, und gelangt schließlich, falls die Funktionen α_ι nicht sämtlich verschwinden (ein Fall, welchen wir von dem Modulbegriff ganz ausschließen wollen) zu einer irreduktibeln Basis. Wir werden in der Folge unter einer Basis schlechtweg stets eine irreduktible Basis verstehen.

2. Obwohl man nach dem vorhergehenden für einen und denselben Modul sehr verschiedene irreduktible Basen auffinden kann, so ist doch die Zahl der Funktionen, die in einer solchen enthalten sind, stets dieselbe, da im entgegengesetzten Fall dasjenige Funktionensystem, welches mehr Funktionen enthält, nicht rational irreduktibel sein könnte. Sind also $\alpha_1, \alpha_2, \cdots \alpha_m$; $\beta_1, \beta_2, \cdots \beta_m$ zwei irreduktible Basen desselben Moduls $\mathfrak{a}$, so ist, da sowohl die α_k als die β_k in $\mathfrak{a}$ enthalten sind:

$$\alpha_k = \sum_{1,\,m}^{\iota} p_k^{(\iota)}\, \beta_\iota;\quad \beta_k = \sum_{1,\,m}^{\iota} q_\iota^{(k)}\, \alpha_\iota,$$

worin die Koeffizienten p, q ganze rationale Funktionen von z sind. Hieraus aber folgt:

$$\sum_{1,\,m}^{\iota} q_\iota^{(k)}\, p_\iota^{(h)} = 0 \text{ oder } 1,$$

---

ist, so folgt:

$$\begin{vmatrix} y_{1,1}, & y_{2,1}, & \cdots & y_{m-1,1}, & y_{m,1} \\ \frac{x\,y_{1,1}}{\partial}, & \frac{x\,y_{2,1}}{\partial}, & \cdots & \frac{x\,y_{m-1,1}}{\partial} & y \\ y_{1,3}, & y_{2,3}, & \cdots & y_{m-1,3}, & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{1,m} & y_{2,m}, & \cdots & y_{m-1\,m}, & 0 \end{vmatrix} = 1.$$

je nachdem h von k verschieden ist oder nicht, und daraus:

$$\sum \pm p_1^{(1)} p_2^{(2)} \cdots p_m^{(m)} \cdot \sum \pm q_1^{(1)} q_2^{(2)} \cdots q_m^{(m)} = 1,$$

und da beide Determinanten ganze rationale Funktionen von z sind, so müssen sie beide konstant sein.

3. Definition. Ein Modul $\mathfrak{a}$ heißt durch einen Modul $\mathfrak{b}$ teilbar, oder $\mathfrak{b}$ ein Teiler (Divisor) von $\mathfrak{a}$, $\mathfrak{a}$ ein Vielfaches (Multiplum) von $\mathfrak{b}$ ($\mathfrak{b}$ geht in $\mathfrak{a}$ auf), wenn jede Funktion in $\mathfrak{a}$ zugleich in $\mathfrak{b}$ enthalten ist. $\mathfrak{b}$ soll ein echter Teiler von $\mathfrak{a}$ heißen, wenn $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar, aber nicht mit $\mathfrak{b}$ identisch ist*).

Aus dieser Definition ergibt sich sofort:

Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, $\mathfrak{b}$ teilbar durch $\mathfrak{c}$, so ist auch $\mathfrak{a}$ teilbar durch $\mathfrak{c}$.

4. Definition. Der Inbegriff $\mathfrak{m}$ aller derjenigen Funktionen, welche zugleich in zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, bildet, falls er nicht aus der einzigen Funktion „Null" besteht, einen Modul (nach der allgemeinen Definition), welcher das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ heißt, weil jeder Modul, welcher ein Vielfaches zugleich von $\mathfrak{a}$ und von $\mathfrak{b}$ ist, auch ein Vielfaches von $\mathfrak{m}$ ist. Das kleinste gemeinschaftliche Vielfache von einer beliebigen Zahl von Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\cdots$ ist dementsprechend der Inbegriff aller der Funktionen, die zugleich in $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\cdots$ enthalten sind. Man kann dasselbe bilden, indem man nach Belieben je zwei der Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\cdots$ durch ihr kleinstes gemeinschaftliches Vielfache ersetzt.

5. Definition. Ist α eine beliebige Funktion in $\mathfrak{a}$, β eine beliebige Funktion in $\mathfrak{b}$, so bildet der Inbegriff aller Funktionen von der Form $\alpha + \beta$ einen Modul $\mathfrak{d}$, welcher der größte gemeinschaftliche Teiler der beiden Moduln $\mathfrak{a}$ und $\mathfrak{b}$ heißt. Derselbe ist, wenn $\mathfrak{a}$ und $\mathfrak{b}$ endliche Moduln sind, selbst ein solcher. Ist nämlich

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_r],\ \mathfrak{b} = [\beta_1, \beta_2, \cdots \beta_s],$$

so ist

$$\mathfrak{d} = [\alpha_1, \alpha_2, \cdots \alpha_r, \beta_1, \beta_2, \cdots \beta_s].$$

Nach der Definition der Teilbarkeit ist $\mathfrak{d}$ ein Teiler sowohl von $\mathfrak{a}$ als von $\mathfrak{b}$. Ist umgekehrt $\mathfrak{d}'$ ein Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$, so sind die Funktionen α sowohl als die Funktionen β, mithin auch die Funktionen $\alpha + \beta$ in $\mathfrak{d}'$ enthalten; daher ist $\mathfrak{d}$ durch $\mathfrak{d}'$ teilbar.

*) Der Begriff der Teilbarkeit der Moduln ist der von den Zahlen her gewohnten Anschauung zuwider gebildet, insofern der Teiler einen größeren Inhalt an Funktionen enthält als das Vielfache.

Die Definition des größten gemeinschaftlichen Teilers einer beliebigen Anzahl von Moduln ergibt sich hiernach von selbst.

6. Definition. Ist $\mathfrak{a}$ ein Modul, α jede Funktion in $\mathfrak{a}$ und μ eine beliebige Funktion in Ω, so verstehen wir unter dem Produkt $\mu\mathfrak{a}$ oder $\mathfrak{a}\mu$ den Inbegriff aller Funktionen $\mu\alpha$, welcher wieder ein Modul ist. Ist

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_r]$$

ein endlicher Modul, so ist

$$\mu\mathfrak{a} = [\mu\alpha_1, \mu\alpha_2, \cdots \mu\alpha_r],$$

also ebenfalls ein endlicher Modul, und aus $\mu\mathfrak{a} = \mu\mathfrak{b}$ folgt $\mathfrak{a} = \mathfrak{b}$, wenn μ von Null verschieden ist.

7. Definition. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Moduln, α, β sämtliche Funktionen in $\mathfrak{a}$, resp. in $\mathfrak{b}$, so verstehen wir unter dem Produkt

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} = \mathfrak{c}$$

den Inbegriff aller Produkte einer Funktion α und einer Funktion β und aller Summen solcher Produkte, also sämtlicher Funktionen, welche durch das Zeichen

$$\gamma = \sum \alpha\beta$$

bezeichnet werden können.

Dieses Funktionensystem bildet jederzeit einen Modul, und zwar einen endlichen, wenn $\mathfrak{a}$ und $\mathfrak{b}$ solche sind. Sind nämlich $\mathfrak{a}$ und $\mathfrak{b}$ so definiert, wie in 5., so bilden die $r \cdot s$ Funktionen $\alpha_\varkappa \beta_\lambda$ eine, wenn auch reduktible, Basis von $\mathfrak{c}$. Ein Produkt aus beliebig vielen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\cdots$ erklärt sich hiernach von selbst, und es gilt für dasselbe der Fundamentalsatz der Multiplikation von der Vertauschbarkeit der Faktoren. Sind die einzelnen Funktionen eines solchen Produkts, deren Anzahl m sei, einander gleich und $= \mathfrak{a}$, so wird dasselbe mit $\mathfrak{a}^m$ bezeichnet, und es ist

$$\mathfrak{a}^{m+m'} = \mathfrak{a}^m \mathfrak{a}^{m'}.$$

Im allgemeinen ist ein Produkt $\mathfrak{a}\mathfrak{b}$ nicht durch $\mathfrak{a}$ teilbar. Dagegen gilt der Satz, dessen Beweis sich unmittelbar aus der Definition ergibt:

Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}_1$, $\mathfrak{b}$ durch $\mathfrak{b}_1$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}_1\mathfrak{b}_1$.

8. Definition. Unter dem Quotienten $\frac{\mathfrak{b}}{\mathfrak{a}}$ zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ soll der Inbegiff aller derjenigen Funktionen γ verstanden werden, welche die Eigenschaft haben, daß $\gamma\mathfrak{a}$ durch $\mathfrak{b}$ teilbar ist. Dieser

Quotient ist, falls er nicht aus der einzigen Funktion „Null“ besteht, ein Modul $\mathfrak{c}$, was sofort aus der Definition erhellt. Das Produkt $\frac{\mathfrak{b}}{\mathfrak{a}} \cdot \mathfrak{a}$ ist jederzeit durch $\mathfrak{b}$ teilbar, wenn auch nicht immer gleich $\mathfrak{b}$.

§ 5.

Kongruenzen.

Zwei Funktionen α, β heißen kongruent nach dem Modul $\mathfrak{a}$

$$\alpha \equiv \beta \,(\mathrm{mod.}\,\mathfrak{a}),$$

wenn die Differenz der beiden Funktionen, $\alpha - \beta$, in dem Modul $\mathfrak{a}$ enthalten ist.

Aus dieser Definition ergeben sich unmittelbar die folgenden Sätze:

1. Ist $\alpha \equiv \beta$, $\beta \equiv \gamma$ (mod. $\mathfrak{a}$), so ist $\alpha \equiv \gamma$ (mod. $\mathfrak{a}$).

2. Ist $\mathfrak{b}$ irgendein Teiler von $\mathfrak{a}$, so folgt aus $\alpha \equiv \beta$ (mod. $\mathfrak{a}$), daß auch $\alpha \equiv \beta$ (mod. $\mathfrak{b}$) ist.

3. Ist $\alpha \equiv \beta$ (mod. $\mathfrak{a}$), μ eine beliebige Funktion in Ω, so folgt $\mu\alpha \equiv \mu\beta$ (mod. $\mu\mathfrak{a}$), und umgekehrt folgt aus der letzteren Kongruenz die erstere, wenn μ von Null verschieden.

4. Ist $\alpha \equiv \beta$, $\alpha_1 \equiv \beta_1$ (mod. $\mathfrak{a}$), so ist auch $\alpha \pm \alpha_1 \equiv \beta \pm \beta_1$ (mod. $\mathfrak{a}$).

Sind $\lambda_1, \lambda_2, \cdots \lambda_m$ beliebig gegebene Funktionen in Ω, $c_1, c_2, \cdots c_m$ willkürliche Konstanten, so heißt der Inbegriff aller Funktionen von der Form

$$c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m$$

eine Schar und wird mit $(\lambda_1, \lambda_2, \cdots \lambda_m)$ bezeichnet. Das Funktionensystem $\lambda_1, \lambda_2, \cdots \lambda_m$ heißt die Basis der Schar. Die Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$ heißen linear unabhängig oder ihr System linear irreduktibel, wenn eine Gleichung (Identität) von der Form

$$c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m = 0$$

nicht anders bestehen kann, als wenn die konstanten Koeffizienten $c_1, c_2, \cdots c_m$ alle verschwinden.

Hiernach gilt der Satz, daß jede Schar eine linear irreduktible Basis besitzt. Denn ist $c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m = 0$ und c_1 von Null verschieden, so ist die Schar $(\lambda_1, \lambda_2, \cdots \lambda_m)$ identisch mit der Schar $(\lambda_2, \lambda_3, \cdots \lambda_m)$, deren Basis eine Funktion weniger enthält. Ist diese noch nicht linear irreduktibel, so kann man auf die gleiche Weise weiterschließen. Auch hier soll in der Folge unter einer Basis schlechtweg eine irreduktible Basis verstanden sein. Die Anzahl der Funktionen, welche in einer irreduktiblen Basis einer

Schar enthalten sind, ist stets dieselbe und heißt die Dimension der Schar. Ist m die Dimension, so heißt die Schar auch eine m-fache. Irgend m Funktionen einer solchen Schar bilden eine irreduktible Basis derselben dann und nur dann, wenn sie linear unabhängig sind.

Die Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$ heißen linear unabhängig in bezug auf den Modul $\mathfrak{a}$, wenn eine Kongruenz von der Form

$$c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m \equiv 0 \pmod{\mathfrak{a}}$$

für keine anderen als verschwindende konstante Koeffizienten c_1, $c_2, \cdots c_m$ besteht. Zwei Summen von der Form $\sum c_\iota \lambda_\iota$ mit verschiedenen Werten der konstanten Koeffizienten c_ι sind dann auch stets inkongruent nach dem Modul $\mathfrak{a}$.

Es seien nun $\mathfrak{a}$ und $\mathfrak{b}$ zwei Moduln, und es werde zunächst angenommen, es existieren in $\mathfrak{b}$ nur eine endliche Anzahl von Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$, welche nach dem Modul $\mathfrak{a}$ linear unabhängig sind. Jede Funktion β in $\mathfrak{b}$ genügt dann einer und nur einer Kongruenz von der Form

$$\beta \equiv c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m \pmod{\mathfrak{a}}$$

mit konstanten Koeffizienten $c_1, c_2, \cdots c_m$. Die Schar $(\lambda_1, \lambda_2, \cdots \lambda_m)$ kann daher ein vollständiges Restsystem des Moduls $\mathfrak{b}$ nach dem Modul $\mathfrak{a}$ und $\lambda_1, \lambda_2, \cdots \lambda_m$ eine Basis desselben genannt werden, und man kann in symbolischer Bezeichnung setzen:

$$\mathfrak{b} \equiv (\lambda_1, \lambda_2, \cdots \lambda_m) \pmod{\mathfrak{a}}.$$

Wählt man in $\mathfrak{b}$ irgendein System von m Funktionen $\lambda_1', \lambda_2', \cdots \lambda_m'$ aus, so gelten m Kongruenzen

$$\lambda_h' \equiv \sum_\iota^\iota k_{h,\iota}\,\lambda_\iota \pmod{\mathfrak{a}}$$

mit konstanten $k_{h,\iota}$, und dies System bildet dann und nur dann eine Basis eines vollständigen Restsystems von $\mathfrak{b}$ nach $\mathfrak{a}$, wenn die Determinante

$$\sum \pm k_{1,1}\, k_{2,2} \cdots k_{m,m}$$

von Null verschieden ist.

§ 6.

Norm eines Moduls in bezug auf einen andern.

Ist $(\lambda_1, \lambda_2, \cdots \lambda_m)$ ein beliebiges vollständiges Restsystem eines Moduls $\mathfrak{b}$ in bezug auf einen andern $\mathfrak{a}$, so ergibt sich, weil $z\mathfrak{b}$ durch $\mathfrak{b}$

teilbar ist, ein ganz bestimmtes System von m^2 Konstanten $c_{h,k}$, durch welches die Kongruenzen erfüllt werden:

$$\left.\begin{aligned} z\,\lambda_1 &\equiv c_{1,1}\,\lambda_1 + c_{2,1}\,\lambda_2 + \cdots + c_{m,1}\,\lambda_m \\ z\,\lambda_2 &\equiv c_{1,2}\,\lambda_1 + c_{2,2}\,\lambda_2 + \cdots + c_{m,2}\,\lambda_m \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ z\,\lambda_m &\equiv c_{1,m}\,\lambda_1 + c_{2,m}\,\lambda_2 + \cdots + c_{m,m}\,\lambda_m \end{aligned}\right\} \pmod{\mathfrak{a}}$$

und durch Auflösung dieses Systems erkennt man, daß jede Funktion λ_i, und mithin jede Funktion β des Moduls $\mathfrak{b}$ durch Multiplikation mit der ganzen rationalen Funktion m^{ten} Grades von z

$$(\mathfrak{b},\mathfrak{a}) = (-1)^m \begin{vmatrix} c_{1,1} - z, & c_{2,1}, & \cdots & c_{m,1} \\ c_{1,2}, & c_{2,2} - z, & \cdots & c_{m,2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1,m}, & c_{2,m}, & \cdots & c_{m,m} - z \end{vmatrix}$$

in eine Funktion des Moduls $\mathfrak{a}$ verwandelt wird. Diese Funktion $(\mathfrak{b},\mathfrak{a})$ ist, wie sich aus dem Multiplikationssatz der Determinanten leicht ergibt, von der Wahl der Basis $\lambda_1, \lambda_2, \cdots \lambda_m$ unabhängig, also nur von den beiden Moduln $\mathfrak{a}$, $\mathfrak{b}$ abhängig und soll die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{b}$ genannt werden.

Ist jede Funktion in $\mathfrak{b}$ zugleich in $\mathfrak{a}$ enthalten, also $\mathfrak{b}$ durch $\mathfrak{a}$ teilbar, so ist $m = 0$ und $(\mathfrak{b},\mathfrak{a}) = 1$ zu setzen. Wenn dagegen $\mathfrak{b}$ nicht, wie oben angenommen, eine endliche Anzahl in bezug auf $\mathfrak{a}$ linear unabhängiger Funktionen enthält, dann soll festgesetzt werden, daß $(\mathfrak{b},\mathfrak{a}) = 0$ sei.

1. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{d}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, so ist jede Kongruenz zwischen Funktionen des Moduls $\mathfrak{b}$ in bezug auf den Modul $\mathfrak{a}$ vollkommen gleichbedeutend mit der Kongruenz derselben Funktionen nach dem Modul $\mathfrak{m}$; andererseits ist jede Funktion in $\mathfrak{b}$ einer Funktion in $\mathfrak{d}$ und umgekehrt jede Funktion in $\mathfrak{d}$ einer Funktion in $\mathfrak{b}$ kongruent nach dem Modul $\mathfrak{a}$. Aus diesen Bemerkungen ergibt sich sofort der wichtige Satz:

$$(\mathfrak{b},\mathfrak{a}) = (\mathfrak{b},\mathfrak{m}) = (\mathfrak{d},\mathfrak{a}),$$

welcher auch richtig bleibt, wenn $(\mathfrak{b},\mathfrak{a}) = 0$ ist.

2. Ist der Modul $\mathfrak{a}$ teilbar durch den Modul $\mathfrak{b}$, dieser durch den dritten Modul $\mathfrak{c}$, so ist

$$(\mathfrak{c},\mathfrak{a}) = (\mathfrak{c},\mathfrak{b})(\mathfrak{b},\mathfrak{a}).$$

Der Satz ist offenbar richtig, wenn von den beiden Normen $(\mathfrak{c}, \mathfrak{b})$, $(\mathfrak{b}, \mathfrak{a})$ eine verschwindet. Ist dies nicht der Fall und ist

$$\mathfrak{c} \equiv (\varrho_1, \varrho_2, \cdots \varrho_r) \pmod{\mathfrak{b}},$$
$$\mathfrak{b} \equiv (\lambda_1, \lambda_2, \cdots \lambda_s) \pmod{\mathfrak{a}},$$

so sind die Funktionen $\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s$ zusammengenommen linear unabhängig nach dem Modul $\mathfrak{a}$; denn ist

$$\sum^{\iota} c_\iota \varrho_\iota + \sum^{\iota} c'_\iota \lambda_\iota \equiv 0 \pmod{\mathfrak{a}},$$

so folgt, da $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar ist und die Funktionen λ_ι in $\mathfrak{b}$ enthalten sind,

$$\sum^{\iota} c_\iota \varrho_\iota \equiv 0 \pmod{\mathfrak{b}}, \text{ mithin } c_\iota = 0,$$
$$\sum^{\iota} c'_\iota \lambda_\iota \equiv 0 \pmod{\mathfrak{a}}, \text{ mithin } c'_\iota = 0.$$

Da ferner jede Funktion γ in $\mathfrak{c}$ einer Kongruenz von der Form genügt:

$$\gamma \equiv \sum c_\iota \varrho_\iota + \sum c'_\iota \lambda_\iota \pmod{\mathfrak{a}},$$

so ist die $(r+s)$-fache Schar $(\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s)$ ein vollständiges Restsystem von $\mathfrak{c}$ nach $\mathfrak{a}$, oder

$$\mathfrak{c} \equiv (\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s) \pmod{\mathfrak{a}}.$$

Ist daher

$$z\varrho_1 = e_{1,1}\varrho_1 + \cdots + e_{r,1}\varrho_r + \beta_1$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$z\varrho_r = e_{1,r}\varrho_1 + \cdots + e_{r,r}\varrho_r + \beta_r,$$

worin die $e_{\iota,\varkappa}$ Konstanten, die β_ι Funktionen in $\mathfrak{b}$ sind, also:

$$(\mathfrak{c}, \mathfrak{b}) = (-1)^r \begin{vmatrix} e_{1,1} - z, & \cdots e_{r,1} \\ \cdots\cdots\cdots & \\ e_{1,r}, & \cdots e_{r,r} - z \end{vmatrix},$$

ferner:

$$\left.\begin{aligned} \beta_1 &\equiv h_{1,1}\lambda_1 + \cdots + h_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots\cdots \\ \beta_r &\equiv h_{1,r}\lambda_1 + \cdots + h_{s,r}\lambda_s \\ z\lambda_1 &\equiv c_{1,1}\lambda_1 + \cdots + c_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots\cdots \\ z\lambda_s &\equiv c_{1,s}\lambda_1 + \cdots + c_{s,s}\lambda_s \end{aligned}\right\} \pmod{\mathfrak{a}}$$

mit konstanten Koeffizienten $h_{\iota,\varkappa}$, $c_{\iota,\varkappa}$, also

$$(\mathfrak{b}, \mathfrak{a}) = (-1)^s \begin{vmatrix} c_{1,1} - z, & \cdots c_{s,1} \\ \cdots\cdots\cdots & \\ c_{1,s}, & \cdots c_{s,s} - z \end{vmatrix},$$

so folgt:

$$\left.\begin{aligned} z\varrho_1 &\equiv e_{1,1}\varrho_1 + \cdots + e_{r,1}\varrho_r + h_{1,1}\lambda_1 + \cdots + h_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z\varrho_r &\equiv e_{1,r}\varrho_1 + \cdots + e_{r,r}\varrho_r + h_{1,r}\lambda_1 + \cdots + h_{s,r}\lambda_s \\ z\lambda_1 &\equiv c_{1,1}\lambda_1 + \cdots + c_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z\lambda_s &\equiv c_{1,s}\lambda_1 + \cdots + c_{s,s}\lambda_s \end{aligned}\right\} \text{(mod. } \mathfrak{a}\text{)}$$

und hieraus

$$(\mathfrak{c},\mathfrak{a}) = (-1)^{r+s}\begin{vmatrix} e_{1,1}-z, \cdots e_{r,1}, & h_{1,1}, & \cdots h_{s,1} \\ \cdots\cdots\cdots\cdots & \cdots\cdots & \cdots\cdots \\ e_{1,r}, \cdots e_{r,r}-z, & h_{1,r}, & \cdots h_{s,r} \\ 0 \cdots 0 & c_{1,1}-z, & \cdots c_{s,1} \\ \cdots\cdots\cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 \cdots 0 & c_{1,s}, & \cdots c_{s,s}-z \end{vmatrix} = (\mathfrak{c},\mathfrak{b})\,(\mathfrak{b},\mathfrak{a}).$$

3. Wenn die Basis-Funktionen $\beta_1, \beta_2, \cdots \beta_s$ eines endlichen Moduls $\mathfrak{b} = [\beta_1, \beta_2, \cdots \beta_s]$ durch Multiplikation mit von Null verschiedenen ganzen rationalen Funktionen von z in Funktionen eines Moduls $\mathfrak{a}$ verwandelt werden können, so ist die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{b}$, $(\mathfrak{b},\mathfrak{a})$ von Null verschieden. Zugleich ist das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ ein endlicher Modul $\mathfrak{m}$, von dem eine irreduktible Basis in der Form angenommen werden kann:

$$\begin{aligned} \mu_1 &= a_{1,1}\beta_1, \\ \mu_2 &= a_{1,2}\beta_1 + a_{2,2}\beta_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \mu_s &= a_{1,s}\beta_1 + a_{2,s}\beta_2 + \cdots + a_{s,s}\beta_s, \end{aligned}$$

worin die Koeffizienten $a_{\iota,\varkappa}$ ganze rationale Funktionen von z sind, und zwar so, daß

$$(\mathfrak{b},\mathfrak{a}) = a_{1,1}\,a_{2,2}\cdots a_{s,s}.$$

Zum Beweise dieses wichtigen Theorems nehmen wir an, es sei $\mathfrak{a}_1$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $[\beta_1]$, $\mathfrak{a}_2$ der von $\mathfrak{a}_1$ und $[\beta_2]$ u. s. f., so daß $\mathfrak{a}_r$ der Inbegriff aller Funktionen von der Form

$$\alpha_r = \alpha + y_1\beta_1 + \cdots + y_r\beta_r$$

ist, wo α eine Funktion in $\mathfrak{a}$, $y_1, \cdots y_r$ ganze rationale Funktionen von z sind. Es ist dann $\mathfrak{a}_s$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$. Da nun jeder Modul $\mathfrak{a}_r$ durch den folgenden $\mathfrak{a}_{r+1}$ teilbar ist, so folgt aus 1. und 2.

$$(\mathfrak{b},\mathfrak{a}) = (\mathfrak{a}_s,\mathfrak{a}) = (\mathfrak{a}_s,\mathfrak{a}_{s-1})\,(\mathfrak{a}_{s-1},\mathfrak{a}_{s-2})\cdots(\mathfrak{a}_1,\mathfrak{a}),$$

und es handelt sich also noch um die Bestimmung von $(\mathfrak{a}_r, \mathfrak{a}_{r-1})$. Es ist aber

$$\alpha_r = \alpha_{r-1} + y_r \beta_r \equiv y_r \beta_r \pmod{\mathfrak{a}_{r-1}},$$

und nach der Voraussetzung gibt es eine von Null verschiedene ganze rationale Funktion x_r von z, für welche

$$x_r \beta_r \equiv 0 \pmod{\mathfrak{a}},$$

also auch

$$x_r \beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}.$$

Ist nun $a_{r,r}$ unter allen der letzteren Kongruenz genügenden Funktionen x_r eine von möglichst niedrigem Grade m_r, die zugleich so angenommen sei, daß der Koeffizient der höchsten Potenz von $z = 1$ ist, so sind alle andern dieser Kongruenz genügenden Funktionen x_r durch $a_{r,r}$ teilbar; denn es ist für ein beliebiges ganzes rationales q

$$(x_r - q\, a_{r,r})\, \beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

und wenn x_r nicht durch $a_{r,r}$ teilbar ist, so läßt sich q so wählen, daß $x_r - q\, a_{r,r}$ von niedrigerem Grade wird als $a_{r,r}$, gegen die Voraussetzung.

Setzt man also

$$y_r = q\, a_{r,r} + b_{r,r}$$

und bestimmt q so, daß der Grad von $b_{r,r}$ kleiner als m_r wird, so folgt:

$$\alpha_r \equiv b_{r,r} \beta_r \pmod{\mathfrak{a}_{r-1}}$$

und hieraus

$$\mathfrak{a}_r \equiv (\beta_r, z\beta_r, \cdots z^{m_r-1}\beta_r) \pmod{\mathfrak{a}_{r-1}}.$$

Wenn man daher für den Augenblick setzt:

$$a_{r,r} = c_0 + c_1 z + \cdots + c_{m_r-1} z^{m_r-1} + z^{m_r},$$

$$\lambda_k = z^{k-1}\beta_r,$$

so folgt:

$$z\lambda_1 = \lambda_2,\ z\lambda_2 = \lambda_3 \cdots$$

$$z\lambda_{m_r} \equiv -c_0\lambda_1 - c_1\lambda_2 - \cdots - c_{m_r-1}\lambda_{m_r} \pmod{\mathfrak{a}_{r-1}}$$

also:

$$(\mathfrak{a}_r, \mathfrak{a}_{r-1}) = (-1)^{m_r} \begin{vmatrix} -z, & 1, & 0, \cdots & 0 \\ 0, & -z, & 1, \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0, & 0, & 0, \cdots & 1 \\ -c_0, & -c_1, & -c_2, \cdots & -c_{m_r-1} - z \end{vmatrix} = a_{r,r}.$$

Hieraus ergibt sich wie in 2., daß das Funktionensystem

$$\beta_1,\ z\,\beta_1,\ \cdots\ z^{m_1-1}\,\beta_1,$$
$$\beta_2,\ z\,\beta_2,\ \cdots\ z^{m_2-1}\,\beta_2,$$
$$\cdots\cdots\cdots\cdots$$
$$\beta_s,\ z\,\beta_s,\ \cdots\ z^{m_s-1}\,\beta_s,$$

eine Basis eines vollständigen Restsystems von $\mathfrak{b}$ nach $\mathfrak{a}$ bildet, und daß

$$(\mathfrak{b},\mathfrak{a}) = \mathfrak{a}_{1,1}\,\mathfrak{a}_{2,2}\cdots\mathfrak{a}_{s,s}$$

vom Grade

$$m = m_1 + m_2 + \cdots + m_s$$

ist.

Da nun $\mathfrak{a}_{r,r}\,\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}$, so läßt sich eine Funktion μ_r in $\mathfrak{a}$ und ganze rationale Funktionen $a_{k,r}$ so bestimmen, daß

$$\mu_r = a_{1,r}\,\beta_1 + a_{2,r}\,\beta_2 + \cdots + a_{r,r}\,\beta_r$$

wird; die auf diese Weise bestimmten Funktionen

$$\mu_1 = a_{1,1}\,\beta_1,$$
$$\mu_2 = a_{1,2}\,\beta_1 + a_{2,2}\,\beta_2$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mu_s = a_{1,s}\,\beta_1 + a_{2,s}\,\beta_2 + \cdots + a_{s,s}\,\beta_s$$

sind, da keine der Funktionen $a_{1,1}, \cdots a_{s,s}$ verschwindet, rational unabhängig und sind sämtlich zugleich in $\mathfrak{a}$ und in $\mathfrak{b}$, also auch in dem kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ dieser beiden Moduln enthalten. Es ist noch nachzuweisen, daß dieselben eine Basis von $\mathfrak{m}$ bilden.

Es sei $\mathfrak{m}_r$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $[\beta_1, \beta_2, \cdots \beta_r]$, $\mathfrak{m}_s = \mathfrak{m}$, so daß unter den Moduln $\mathfrak{m}_1, \mathfrak{m}_2, \cdots \mathfrak{m}_s$ jeder durch alle folgenden, als auch durch $\mathfrak{m}$ teilbar ist, und

$$\nu_r = z_1\,\beta_1 + z_2\,\beta_2 + \cdots + z_r\,\beta_r$$

eine Funktion in $\mathfrak{m}_r$, also auch in $\mathfrak{a}$.

Es ist hiernach

$$z_r\,\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

also

$$z_r = x_r\,\mathfrak{a}_{r,r},$$

worin x_r eine ganze rationale Funktion bedeutet. Daher ist

$$\nu_r - x_r\,\mu_r \equiv 0 \pmod{\mathfrak{m}_{r-1}},\quad \nu_1 - x_1\,\mu_1 = 0,$$

woraus folgt:

$$\nu_r = x_1\,\mu_1 + x_2\,\mu_2 + \cdots + x_r\,\mu_r,$$

also:

$$\mathfrak{m}_r = [\mu_1,\ \mu_2, \cdots \mu_r],$$
$$\mathfrak{m} = [\mu_1,\ \mu_2, \cdots \mu_s],$$

w. z. b. w.

Hiernach enthält eine irreduktible Basis des Moduls $\mathfrak{m}$ genau ebenso viele Funktionen wie eine irreduktible Basis von $\mathfrak{b}$. Wählt man statt der Basis $\mu_1, \mu_2, \cdots \mu_s$ eine andere $\mu'_1, \mu'_2 \cdots \mu'_s$, so läßt sich $\mu'_1, \mu'_2, \cdots \mu'_s$ in der Form ausdrücken

$$\mu'_k = a'_{1,k}\beta_1 + a'_{2,k}\beta_2 + \cdots + a'_{s,k}\beta_s$$

mit ganzen rationalen Koeffizienten $a'_{i,k}$, und aus § 4, 2. ergibt sich

$$(\mathfrak{b}, \mathfrak{a}) = \text{konst.} \sum \pm a'_{1,1} a'_{2,2} \cdots a'_{s,s}.$$

4. Machen wir insbesondere die Annahme, es sei $\mathfrak{a}$ gleichfalls ein endlicher Modul, der eine irreduktible Basis von ebenso vielen Funktionen besitzt wie $\mathfrak{b}$, und es sei außerdem $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, dann lassen sich, wenn

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_s]$$

ist, die ganzen rationalen Funktionen $b_{i,k}$ von z so bestimmen, daß

$$\alpha_k = b_{1,k}\beta_1 + b_{2,k}\beta_2 + \cdots + b_{s,k}\beta_s,$$

und die Voraussetzung von 3., daß die Funktionen β_i durch Multiplikation mit ganzen rationalen Funktionen von z in Funktionen des Moduls $\mathfrak{a}$ verwandelt werden können, ist erfüllt, wie man durch Auflösung dieses Gleichungssystems erkennt. Zugleich ist hier $\mathfrak{a}$ selbst das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$, und daraus ergibt sich

$$(\mathfrak{b}, \mathfrak{a}) = \text{konst.} \sum \pm b_{1,1} b_{2,2} \cdots b_{n,n}.$$

5. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ und ν eine beliebige Funktion in Ω, so ist, wie sich aus der Definition ohne Schwierigkeit ergibt, $\nu\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache von $\nu\mathfrak{a}$ und $\nu\mathfrak{b}$. Ist $(\mathfrak{b}, \mathfrak{a}) = 0$, so ist auch $(\nu\mathfrak{b}, \nu\mathfrak{a}) = 0$. Ist aber $(\mathfrak{b}, \mathfrak{a})$ und ν von Null verschieden, so ergibt sich

$$(\nu\mathfrak{b}, \nu\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a}),$$

wenn man in 3. die Basis-Funktionen μ_i, β_i von $\mathfrak{m}$ und $\mathfrak{b}$ durch $\nu\mu_i$, $\nu\beta_i$ ersetzt.

§ 7.

Die Ideale in $\mathfrak{o}$.

Ein System $\mathfrak{a}$ von **ganzen** Funktionen von z im Körper Ω heißt ein **Ideal**, wenn es die beiden folgenden Bedingungen erfüllt:

I. Summe und Differenz je zweier Funktionen in $\mathfrak{a}$ ergeben wieder eine Funktion in $\mathfrak{a}$.

II. Das Produkt einer jeden Funktion in $\mathfrak{a}$ mit einer jeden Funktion in $\mathfrak{o}$ (§ 3) ist wieder eine Funktion in $\mathfrak{a}$.

Jedes Ideal ist also zugleich ein Modul und alle für die Moduln erklärten Begriffe und Bezeichnungen können auf die Ideale angewandt werden.

Der Modul $\mathfrak{o}$ (das System aller ganzen Funktionen von z) ist selbst ein Ideal, und jedes Ideal ist durch $\mathfrak{o}$ teilbar. Ebenso ist, wenn μ eine beliebige von Null verschiedene Funktion von $\mathfrak{o}$ bedeutet, der Modul $\mathfrak{o}\mu$ (das System aller durch μ teilbaren ganzen Funktionen) ein Ideal. Ein solches Ideal soll ein Hauptideal genannt werden. Ist $\omega_1, \omega_2, \ldots \omega_n$ eine Basis von $\mathfrak{o}$, so ist

$$\mathfrak{o}\mu = [\omega_1\mu, \omega_2\mu, \ldots \omega_n\mu]$$

und $\mathfrak{o}\mu$ ist das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}$ und $\mathfrak{o}\mu$. Daher ist nach § 6, 4. und nach der Definition (4.) in § 2:

$$(1) \qquad (\mathfrak{o}, \mathfrak{o}\mu) = \text{konst. } N(\mu)$$

und mithin von Null verschieden.

Ist $\mathfrak{a}$ irgend ein Ideal und α eine beliebige Funktion in $\mathfrak{a}$, so ist (wegen II.) das Hauptideal $\mathfrak{o}\alpha$ teilbar durch $\mathfrak{a}$, und mithin nach § 6, 2.:

$$(2) \qquad (\mathfrak{o}, \mathfrak{o}\alpha) = (\mathfrak{o}, \mathfrak{a})\ (\mathfrak{a}, \mathfrak{o}\alpha),$$

mithin auch $(\mathfrak{o}, \mathfrak{a})$ von Null verschieden. Da nun wieder $\mathfrak{a}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}$ ist, so besitzt $\mathfrak{a}$ nach § 6, 3. eine irreduktible Basis, welche aus n ganzen Funktionen $\alpha_1, \alpha_2, \ldots \alpha_n$ besteht, die demnach auch eine Basis des Körpers Ω bilden.

Die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{o}$, d. h. die ganze rationale Funktion $(\mathfrak{o}, \mathfrak{a})$ von z soll die Norm des Ideals $\mathfrak{a}$ genannt und mit $N(\mathfrak{a})$ bezeichnet werden. Der Grad dieser ganzen rationalen Funktion heißt zugleich der Grad des Ideals $\mathfrak{a}$.

Ist

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n], \quad \mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n]$$

und

$$\begin{aligned}
\alpha_1 &= a_{1,1}\omega_1 + a_{2,1}\omega_2 + \cdots + a_{n,1}\omega_n, \\
\alpha_2 &= a_{1,2}\omega_1 + a_{2,2}\omega_2 + \cdots + a_{n,2}\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n &= a_{1,n}\omega_1 + a_{2,n}\omega_2 + \cdots + a_{n,n}\omega_n
\end{aligned}$$

mit ganzen rationalen Koeffizienten $a_{\varkappa,\lambda}$, so ergibt sich aus § 6, 4.:

$$(3) \qquad N(\mathfrak{a}) = \text{konst.} \sum \pm a_{1,1}\, a_{2,2} \cdots a_{n,n}.$$

Da jede Funktion in $\mathfrak{o}$, also auch die Funktion „1“ durch Multiplikation mit $N(\mathfrak{a})$ in eine Funktion des Ideals $\mathfrak{a}$ verwandelt wird, so ist $N(\mathfrak{a})$ stets eine Funktion in $\mathfrak{a}$.

Die Norm des Ideals $\mathfrak{o}$ ist gleich 1 und umgekehrt ist $\mathfrak{o}$ das einzige Ideal, welches diese Eigenschaft hat. Auch ist $\mathfrak{o}$ das einzige Ideal, welches die Funktion „1“ (oder eine Konstante) enthält.

Ist α eine Funktion in $\mathfrak{a}$, so folgt aus (1), (2), (3):

$$N(\alpha) = \text{konst.}\, N(\mathfrak{a})\,(\mathfrak{a}, \mathfrak{o}\alpha), \tag{4}$$

d. h. die Norm einer jeden in $\mathfrak{a}$ enthaltenen Funktion ist durch die Norm von $\mathfrak{a}$ teilbar.

Für die Kongruenzen in bezug auf einen Idealmodul gilt der folgende Satz, welcher die Ideale wesentlich von den allgemeinen Moduln unterscheidet.

Sind μ, μ_1, ν, ν_1 Funktionen in $\mathfrak{o}$, welche den Kongruenzen genügen

$$\mu \equiv \mu_1, \quad \nu \equiv \nu_1 \pmod{\mathfrak{a}},$$

so ist auch

$$\mu\nu \equiv \mu_1\nu_1 \pmod{\mathfrak{a}}.$$

§ 8.

Multiplikation und Teilung der Ideale.

Aus den Grundeigenschaften I., II. der Ideale und aus den Begriffsbestimmungen in § 4 ergibt sich zunächst:

1. Das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler, das Produkt von zwei (und also auch von beliebig vielen) Idealen sind selbst Ideale. Ebenso ist, wenn ν eine Funktion in $\mathfrak{o}$, $\mathfrak{a}$ ein Ideal ist, das Produkt $\mathfrak{a}\nu$ ein Ideal.

2. Das Produkt aus mehreren Idealen ist durch jeden seiner Faktoren teilbar, und es ist für jedes Ideal $\mathfrak{a}$.

$$\mathfrak{a}\,\mathfrak{o} = \mathfrak{a};$$

denn nach I., II. ist jede Funktion in $\mathfrak{a}\,\mathfrak{o}$ zugleich eine Funktion in $\mathfrak{a}$, und, da $\mathfrak{o}$ die Funktion „1“ enthält, auch umgekehrt jede Funktion in $\mathfrak{a}$ zugleich eine Funktion in $\mathfrak{a}\,\mathfrak{o}$.

3. Ein Hauptideal $\mathfrak{o}\mu$ ist dann und nur dann teilbar durch ein Hauptideal $\mathfrak{o}\nu$, wenn die ganze Funktion μ teilbar ist durch die ganze Funktion ν.

Wir fügen noch folgende Definitionen hinzu:

4. **Definition.** Eine Funktion α in $\mathfrak{o}$ soll durch das Ideal $\mathfrak{a}$ **teilbar heißen**, wenn das Hauptideal $\mathfrak{o}\alpha$ durch $\mathfrak{a}$ teilbar, oder, was **dasselbe sagt, wenn** α eine Funktion in $\mathfrak{a}$ ist.

5. Definition. Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen relativ prim, wenn ihr größter gemeinschaftlicher Teiler $\mathfrak{o}$ ist. Die notwendige und hinreichende Bedingung dafür ist, daß in $\mathfrak{a}$ eine Funktion α, in $\mathfrak{b}$ eine Funktion β existiert der Art, daß

$$\alpha + \beta = 1,$$

oder, anders ausgedrückt, daß in $\mathfrak{a}$ eine der Kongruenz $\alpha \equiv 1 \pmod{\mathfrak{b}}$ oder in $\mathfrak{b}$ eine der Kongruenz $\beta \equiv 1 \pmod{\mathfrak{a}}$ genügende Funktion existiert.

6. Definition. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heißt ein Primideal, wenn kein anderes Ideal außer $\mathfrak{p}$ und $\mathfrak{o}$ in $\mathfrak{p}$ aufgeht.

Auf Grund dieser Definitionen ergeben sich nun die folgenden Sätze über die Teilbarkeit der Ideale.

7. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Ideale mit dem kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ und dem größten gemeinschaftlichen Teiler $\mathfrak{b}$, so folgt aus § 6, 1., 2.

$$N(\mathfrak{m}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{m}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{a}),$$
$$N(\mathfrak{a}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{a}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{a}),$$

folglich $(\mathfrak{b}, \mathfrak{a})$ von Null verschieden und

$$N(\mathfrak{a})\,N(\mathfrak{b}) = N(\mathfrak{m})\,N(\mathfrak{b}).$$

8. Ist das Ideal $\mathfrak{a}$ teilbar durch das Ideal $\mathfrak{b}$, so ist, nach § 6, 2.

$$N(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\,N(\mathfrak{b}),$$

also $N(\mathfrak{a})$ teilbar durch $N(\mathfrak{b})$.

Ist insbesondere $(\mathfrak{b}, \mathfrak{a}) = 1$, so ist auch $\mathfrak{b}$ teilbar durch $\mathfrak{a}$, und es folgt:

9. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$ und ist zugleich $N(\mathfrak{a}) = N(\mathfrak{b})$, so ist $\mathfrak{a} = \mathfrak{b}$, d. h. beide Ideale sind identisch.

10. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}_1$, $\mathfrak{b}$ durch $\mathfrak{b}_1$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}_1\mathfrak{b}_1$ (§ 4, 7.).

11. Ist ein Ideal $\mathfrak{a}$ teilbar durch ein Hauptideal $\mathfrak{o}\mu$, so sind alle Funktionen in $\mathfrak{a}$ von der Form $\beta\mu$, und der Inbegriff der Funktionen β ist wieder ein Ideal $\mathfrak{b}$, so daß man setzen kann

$$\mathfrak{a} = \mu\mathfrak{b}.$$

12. Ist μ eine beliebige von Null verschiedene Funktion in $\mathfrak{o}$ und das Ideal $\mathfrak{a}\mu$ teilbar durch das Ideal $\mathfrak{b}\mu$, so ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, und aus $\mathfrak{a}\mu = \mathfrak{b}\mu$ folgt $\mathfrak{a} = \mathfrak{b}$.

13. Das kleinste gemeinschaftliche Vielfache zweier Ideale $\mathfrak{a}$, $\mathfrak{o}\nu$, davon eines ein Hauptideal ist, hat nach 11. die Form $\mathfrak{r}\nu$, worin $\mathfrak{r}$ ein Ideal ist. Da andererseits $\mathfrak{a}\nu$ ein gemeinschaftliches Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$, also durch $\mathfrak{r}\nu$ teilbar ist, so ist nach 12. $\mathfrak{r}$ ein Teiler von $\mathfrak{a}$.

14. Ist $\mathfrak{a}$ ein Ideal, ν eine Funktion in $\mathfrak{o}$, so ist nach § 6, 2., 5.:

$$(\mathfrak{o}, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)\ (\mathfrak{o}\nu, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)\ (\mathfrak{o}, \mathfrak{a}),$$

also

$$N(\mathfrak{a}\nu) = \text{konst.}\ N(\mathfrak{a})\ N(\nu).$$

Ist also $\mathfrak{r}\nu$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{b}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{a}$, $\mathfrak{o}\nu$, so ergibt sich aus 7.

$$N(\mathfrak{a}) = N(\mathfrak{r})\ N(\mathfrak{b}).$$

15. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist durch ein Primideal $\mathfrak{p}$ teilbar.

Ist nämlich $\mathfrak{a}$ kein Primideal, so hat es mindestens einen von $\mathfrak{o}$ verschiedenen echten Teiler, und von diesen sei $\mathfrak{p}$ ein solcher, dessen Norm von möglichst niedrigem Grade ist. Dieser kann keinen von $\mathfrak{o}$ verschiedenen echten Teiler $\mathfrak{p}'$ haben, denn es wäre auch $\mathfrak{p}'$ ein Teiler von $\mathfrak{a}$ und zugleich (nach 8.) $N(\mathfrak{p}')$ von niedrigerem Grade als $N(\mathfrak{p})$. Dies widerspricht der Voraussetzung über $\mathfrak{p}$, und folglich ist $\mathfrak{p}$ ein Primideal.

16. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{b}$, so ist $\mathfrak{a}\,\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$, und folglich ist jedes durch $\mathfrak{a}$ und durch $\mathfrak{b}$ teilbare Ideal auch durch das Produkt $\mathfrak{a}\,\mathfrak{b}$ teilbar.

Denn nach Voraussetzung gibt es in $\mathfrak{a}$, $\mathfrak{b}$ zwei Funktionen α_1, β_1 der Art, daß

$$\alpha_1 + \beta_1 = 1$$

ist (5.). Ist andererseits $\alpha = \beta$ eine Funktion des kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, so ist hiernach

$$\alpha = \beta = \alpha_1 \beta + \alpha \beta_1,$$

also eine Funktion in $\mathfrak{a}\,\mathfrak{b}$. Es ist demnach $\mathfrak{m}$ teilbar durch $\mathfrak{a}\,\mathfrak{b}$, und da umgekehrt (zufolge 2.) $\mathfrak{a}\,\mathfrak{b}$ durch $\mathfrak{m}$ teilbar ist, so ist $\mathfrak{m}$ mit $\mathfrak{a}\,\mathfrak{b}$ identisch, und aus 7. folgt noch für diesen Fall

$$N(\mathfrak{a}\,\mathfrak{b}) = N(\mathfrak{a})\ N(\mathfrak{b}).$$

17. Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{p}$ ein Primideal, so ist entweder $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar oder $\mathfrak{a}$ relativ prim zu $\mathfrak{p}$; denn da $\mathfrak{p}$ keinen anderen Teiler hat als $\mathfrak{o}$ und $\mathfrak{p}$, so kann auch der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{p}$ kein anderer sein als $\mathfrak{o}$ oder $\mathfrak{p}$.

18. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{b}$ und zu $\mathfrak{c}$, so ist $\mathfrak{a}$ auch relativ prim zu $\mathfrak{bc}$.

Nach Voraussetzung (5.) gibt es in $\mathfrak{b}, \mathfrak{c}$ zwei den Kongruenzen

$$\beta \equiv 1, \quad \gamma \equiv 1 \pmod{\mathfrak{a}}$$

genügende Funktionen, folglich nach § 7

$$\beta\gamma \equiv 1 \pmod{\mathfrak{a}}.$$

Da $\beta\gamma$ in $\mathfrak{bc}$ enthalten ist, so ist hiermit die Behauptung erwiesen.

Es folgt hieraus noch, daß, falls das Produkt $\mathfrak{ab}$ durch ein Primideal teilbar ist, wenigstens einer der beiden Faktoren $\mathfrak{a}, \mathfrak{b}$ durch $\mathfrak{p}$ teilbar sein muß, und, auf Hauptideale angewandt, daß, wenn das Produkt zweier ganzen Funktionen, $\mu\nu$, in $\mathfrak{p}$ enthalten ist, wenigstens der eine der beiden Faktoren μ, ν in $\mathfrak{p}$ enthalten sein muß.

19. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{c}$ und $\mathfrak{ab}$ durch $\mathfrak{c}$ teilbar, so ist $\mathfrak{b}$ durch $\mathfrak{c}$ teilbar. Nach Voraussetzung gibt es in $\mathfrak{a}$ eine Funktion α, welche der Kongruenz genügt

$$\alpha \equiv 1 \pmod{\mathfrak{c}}.$$

Ist nun β eine beliebige Funktion in $\mathfrak{b}$, so ist hiernach

$$\beta \equiv \alpha\beta \text{ und nach Vor. } \equiv 0 \pmod{\mathfrak{c}},$$

folglich β in $\mathfrak{c}$ enthalten, also $\mathfrak{b}$ durch $\mathfrak{c}$ teilbar.

§ 9.

Gesetze der Teilbarkeit der Ideale.

Alle diese Sätze, die sich meist unmittelbar aus der Definition der Ideale ergaben, reichen nicht aus, um die vollständige Analogie zu beweisen, die zwischen den Gesetzen der Teilbarkeit der Ideale und denen der ganzen rationalen Funktionen herrscht. Wir stützen uns bei diesem Beweis auf folgenden Satz:

1. Ist $\mathfrak{a}$ ein Ideal und k eine beliebige ganze rationale Funktion von z, so läßt sich in $\mathfrak{a}$ eine Funktion α so auswählen, daß $(\mathfrak{a}, \mathfrak{o}\alpha)$ mit k keinen Teiler gemeinschaftlich hat*).

Ist nämlich

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n],$$
$$\mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n],$$

*) Die Möglichkeit, diesen Satz schon an dieser Stelle zu beweisen, unterscheidet wesentlich die Theorie der algebraischen Funktionen von der der algebraischen Zahlen und gestattet bei ersterer eine nicht unerhebliche Vereinfachung im Vergleich mit letzterer.

und α eine beliebige Funktion in $\mathfrak{a}$, so lassen sich die ganzen rationalen Funktionen $x_{h,k}$ so bestimmen, daß

$$\begin{aligned}
\alpha\omega_1 &= x_{1,1}\,\alpha_1 + x_{2,1}\,\alpha_2 + \cdots + x_{n,1}\,\alpha_n,\\
\alpha\omega_2 &= x_{1,2}\,\alpha_1 + x_{2,2}\,\alpha_2 + \cdots + x_{n,2}\,\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha\omega_n &= x_{1,n}\,\alpha_1 + x_{2,n}\,\alpha_2 + \cdots + x_{n,n}\,\alpha_n,
\end{aligned}$$

und es ist (§ 6, 4.)

$$(\mathfrak{a},\ \mathfrak{o}\alpha) = \text{konst.}\sum \pm x_{1,1}\,x_{2,2}\cdots x_{n,n}.$$

Ist nun $\sum \pm x_{1,1}\,x_{2,2}\ldots x_{n,n}$ durch einen Linearfaktor $z-c$ von k teilbar, so läßt sich eine nicht durch $z-c$ teilbare Funktion ω in $\mathfrak{o}$ und eine Funktion α' in $\mathfrak{a}$ so bestimmen, daß

$$\alpha\omega = (z-c)\alpha'\text{*)}.$$

Setzt man nun, indem man unter t eine unbestimmte Konstante versteht:

$$t(z-c) - \omega = \omega',$$

so ist

$$N(\omega') = t^n(z-c)^n + a_1 t^{n-1}(z-c)^{n-1} + \cdots + a_{n-1}\,t(z-c) + a_n,$$

worin die von t unabhängigen Koeffizienten $a_1, a_2, \ldots a_n$ ganze rationale Funktionen von z sind. Es kann nun nicht zugleich a_1 durch $z-c$, a_2 durch $(z-c)^2$, ..., a_n durch $(z-c)^n$ teilbar sein, weil sonst gegen die Voraussetzung $\dfrac{\omega}{z-c}$ eine ganze Funktion wäre (§ 2, 5., § 3, 4.). Daher lassen sich nicht alle Glieder von $N(\omega')$ durch $(z-c)^n$ teilen, und wenn also $(z-c)^{n-r}$ die höchste Potenz von $z-c$ ist, durch welche dieselben teilbar sind, so ist $r > 0$ und

$$\frac{N(\omega')}{(z-c)^{n-r}} = t^n(z-c)^r + b_1 t^{n-1} + \cdots + b_{n-1}\,t + b_n = f(t),$$

worin die ganzen rationalen Funktionen $b_1, b_2, \ldots b_n$ nicht alle für $z = c$ verschwinden. Es gibt daher nur eine endliche Anzahl von konstanten Werten t, für welche $f(t)$ durch $z-c$ teilbar ist. Ist

---

*) Wenn nämlich die Determinante $\Sigma \pm x_{1,1}\,x_{2,2}\cdots x_{n,n}$ durch $z-c$ teilbar ist, d. h. für $z = c$ verschwindet, so kann man ein System von Konstanten $c_1, c_2, \ldots c_n$, die nicht sämtlich verschwinden, so bestimmen, daß die ganzen rationalen Funktionen

$$c_1 x_{k,1} + c_2 x_{k,2} + \cdots + c_k x_{k,n} \qquad (k = 1, 2 \ldots n)$$

für $z = c$ verschwinden, also durch $z-c$ teilbar sind, und es ist dann

$$\omega = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n$$

zu setzen.

$z - c'$ ein von $z - c$ verschiedener Linearfaktor von k, so wird $f(t)$ auch nur für eine endliche Anzahl von Werten t durch $z - c'$ teilbar. Daraus folgt, daß man über t so verfügen kann, daß $N(\omega')$ nicht durch $(z-c)^n$ und zugleich durch keinen anderen Linearfaktor von k teilbar wird*). Setzt man, wenn dies geschehen,

$$t\alpha - \alpha' = \alpha'',$$

welches ebenfalls eine Funktion in $\mathfrak{a}$ ist, so folgt

$$\alpha\omega' = (z-c)\alpha'',$$

$$N(\alpha'') = \frac{N(\alpha)\,N(\omega')}{(z-c)^n}$$

und mithin, da nach § 7, (4)

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \text{konst.}\,\frac{N(\alpha)}{N(\mathfrak{a})}$$

ist:

$$(\mathfrak{a}, \mathfrak{o}\alpha'') = \text{konst.}\,\frac{(\mathfrak{a}, \mathfrak{o}\alpha)\,N(\omega')}{(z-c)^n}.$$

Die Funktion $(\mathfrak{a}, \mathfrak{o}\alpha'')$ enthält daher den Faktor $z - c$ mindestens einmal weniger als $(\mathfrak{a}, \mathfrak{o}\alpha)$, während sie zugleich keinen anderen Linearfaktor von k öfter enthält als $(\mathfrak{a}, \mathfrak{o}\alpha)$. Durch wiederholte Anwendung dieses Verfahrens ergibt sich die Richtigkeit des ausgesprochenen Satzes.

2. Jedes Ideal $\mathfrak{a}$ kann als größter gemeinschaftlicher Teiler zweier Hauptideale $\mathfrak{o}\mu$, $\mathfrak{o}\nu$ dargestellt werden, von denen das eine ganz beliebig, nur teilbar durch $\mathfrak{a}$, angenommen werden kann.

Beweis. Man wähle nach Belieben in $\mathfrak{a}$ eine von Null verschiedene Funktion ν, und eine zweite Funktion μ derart, daß die beiden Funktionen $(\mathfrak{a}, \mathfrak{o}\nu)$ und $(\mathfrak{a}, \mathfrak{o}\mu)$ keinen gemeinschaftlichen Teiler haben (nach 1.). Ist nun α eine beliebige Funktion in $\mathfrak{a}$, so ist nach § 6 $(\mathfrak{a}, \mathfrak{o}\mu)\alpha$ in $\mathfrak{o}\mu$, $(\mathfrak{a}, \mathfrak{o}\nu)\alpha$ in $\mathfrak{o}\nu$ enthalten, so daß es zwei Funktionen ω, ω' in $\mathfrak{o}$ gibt, für welche

$$(\mathfrak{a}, \mathfrak{o}\mu)\alpha = \mu\omega, \quad (\mathfrak{a}, \mathfrak{o}\nu)\alpha = \nu\omega'.$$

Wählt man daher, was nach der Voraussetzung über $(\mathfrak{a}, \mathfrak{o}\mu)$, $(\mathfrak{a}, \mathfrak{o}\nu)$ möglich ist, zwei ganze rationale Funktionen g, h von z, welche der Bedingung genügen

$$g(\mathfrak{a}, \mathfrak{o}\mu) + h(\mathfrak{a}, \mathfrak{o}\nu) = 1,$$

so folgt

$$\alpha = g\mu\omega + h\nu\omega',$$

*) Diese Schlüsse gelten in der analogen Frage der Zahlentheorie nicht mehr.

d. h. $\mathfrak{a}$ ist teilbar durch den größten gemeinschaftlichen Teiler von $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$. Und da letzterer umgekehrt durch $\mathfrak{a}$ teilbar ist (weil $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ durch $\mathfrak{a}$ teilbar sind), so ist er gleich $\mathfrak{a}$, w. z. b. w.

3. Jedes Ideal $\mathfrak{a}$ kann durch Multiplikation mit einem Ideal $\mathfrak{m}$ in ein Hauptideal $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}$ verwandelt werden.

Beweis. Man wähle (nach 1.) in $\mathfrak{a}$ eine Funktion μ so, daß $(\mathfrak{a}, \mathfrak{o}\mu)$ keinen Teiler mit $N(\mathfrak{a})$ gemein hat, hierauf eine zweite Funktion ν so, daß $(\mathfrak{a}, \mathfrak{o}\nu)$ mit $(\mathfrak{a}, \mathfrak{o}\mu)$ keinen Teiler gemein hat. Dann ist (nach 2.) $\mathfrak{a}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$. Das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ ist (nach § 8, 13) von der Form $\mathfrak{m}\nu$, worin $\mathfrak{m}$ ein Teiler von $\mathfrak{o}\mu$ ist. Nach § 8, 14 ist alsdann

$$N(\mathfrak{m}) = \frac{N(\mathfrak{o}\mu)}{N(\mathfrak{a})} = (\mathfrak{a}, \mathfrak{o}\mu),$$

also, nach Voraussetzung, ohne gemeinschaftlichen Teiler mit $N(\mathfrak{a})$. Bestimmt man also wieder zwei ganze rationale Funktionen g, h von z, so daß

$$gN(\mathfrak{m}) + hN(\mathfrak{a}) = 1,$$

so folgt aus § 8, 5, da $N(\mathfrak{m})$ in $\mathfrak{m}$, $N(\mathfrak{a})$ in $\mathfrak{a}$ enthalten ist, daß $\mathfrak{m}$ und $\mathfrak{a}$ relative Primideale sind, und daraus, nach § 8, 16.

$$N(\mathfrak{m}\mathfrak{a}) = N(\mathfrak{m})N(\mathfrak{a}) = N(\mathfrak{o}\mu).$$

Da nun $\mathfrak{o}\mu$ durch $\mathfrak{m}$ und durch $\mathfrak{a}$, also auch durch $\mathfrak{m}\mathfrak{a}$ teilbar ist (§ 8, 16.), so ist nach § 8, 9.

$$\mathfrak{m}\mathfrak{a} = \mathfrak{o}\mu,$$

w. z. b. w.*).

4. Ist ein Ideal $\mathfrak{c}$ teilbar durch ein Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$, welches der Bedingung

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}$$

genügt, welches der Quotient von $\mathfrak{c}$ durch $\mathfrak{a}$ heißt.

Ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}\mathfrak{b}'$, so ist $\mathfrak{b}$ teilbar durch $\mathfrak{b}'$, und aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ folgt $\mathfrak{b} = \mathfrak{b}'$.

Beweis. Es sei $\mathfrak{c}$ teilbar durch $\mathfrak{a}$ und (nach 3.) $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$. Es ist alsdann auch $\mathfrak{c}\mathfrak{m}$ teilbar durch $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$ und folglich $\mathfrak{c}\mathfrak{m} = \mathfrak{b}\mu$

*) Man kann das Ideal $\mathfrak{m}$ zugleich so wählen, daß es relativ prim zu einem beliebigen Ideal $\mathfrak{b}$ wird. Dies wird erreicht, wenn man die Funktion μ so annimmt, daß $(\mathfrak{a}, \mathfrak{o}\mu) = N(\mathfrak{m})$ keinen Teiler mit $N(\mathfrak{a})N(\mathfrak{b})$ gemein hat (§ 8, 8.).

(§ 8, 10., 11.); also, durch Multiplikation der letzten Gleichung mit $\mathfrak{a}$,

$$\mathfrak{c}\mu = \mathfrak{a}\mathfrak{b}\mu$$

und nach § 8, 12.

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b},$$

womit der erste Teil des Satzes bewiesen ist*).

Ist ferner $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}\mathfrak{b}'$, so ist (§ 8, 10.) $\mu\mathfrak{b}$ teilbar durch $\mu\mathfrak{b}'$, also $\mathfrak{b}$ durch $\mathfrak{b}'$. — Ist $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$, so folgt $\mu\mathfrak{b} = \mu\mathfrak{b}'$ und mithin $\mathfrak{b} = \mathfrak{b}'$ (§ 8, 12.).

5. Jedes von $\mathfrak{o}$ verschiedene Ideal ist entweder ein Primideal, oder es läßt sich, und nur auf eine Weise, als Produkt von lauter Primidealen darstellen.

Beweis. Ist das Ideal $\mathfrak{a}$ von $\mathfrak{o}$ verschieden, so ist es (§ 8, 15.) durch ein Primideal $\mathfrak{p}_1$ teilbar, und folglich (nach 4.) $= \mathfrak{p}_1\mathfrak{a}_1$, worin $\mathfrak{a}_1$ ein echter Teiler von $\mathfrak{a}$ ist (denn aus $\mathfrak{a}_1 = \mathfrak{a}$ würde nach 4. folgen $\mathfrak{p}_1 = \mathfrak{o}$). Es ist also der Grad von $N(\mathfrak{a}_1)$ niedriger als der von $N(\mathfrak{a})$. Ist $\mathfrak{a}_1$ von $\mathfrak{o}$ verschieden, so schließt man ebenso, daß $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ sein muß, wobei der Grad von $N(\mathfrak{a}_2)$ wieder niedriger ist als der von $N(\mathfrak{a}_1)$. Fährt man auf diese Weise fort, so gelangt man schließlich nach einer endlichen Anzahl von Zerlegungen zu einem Ideal $\mathfrak{a}_{r-1} = \mathfrak{p}_r\mathfrak{a}_r$ derart, daß $N(\mathfrak{a}_r) = 1$, also $\mathfrak{a}_r = \mathfrak{o}$ ist. Es ist daher

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r.$$

Wäre eine solche Zerlegung auf eine zweite Art möglich, etwa

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s,$$

so müßte (§ 8, 18.) von den Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_r$ mindestens eines, etwa $\mathfrak{p}_1$ durch $\mathfrak{q}_1$ teilbar und also $= \mathfrak{q}_1$ sein, also nach 4.

$$\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_r = \mathfrak{q}_2\mathfrak{q}_3 \dots \mathfrak{q}_s.$$

Hieraus schließt man ebenso $\mathfrak{p}_2 = \mathfrak{q}_2$ usf.

Faßt man in der so gewonnenen Zerlegung die einander gleichen Primideale zu Potenzen zusammen, so kann man setzen

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}.$$

Irgendein Teiler $\mathfrak{a}_1$ von $\mathfrak{a}$ kann dann durch kein von $\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_r$ verschiedenes Primideal und durch keines öfter als $\mathfrak{a}$ teilbar sein. Man erhält also die sämtlichen Divisoren von $\mathfrak{a}$, deren Anzahl endlich, und $= (e_1 + 1)(e_2 + 1) \dots (e_r + 1)$ ist, wenn man in

$$\mathfrak{p}_1^{h_1}\mathfrak{p}_2^{h_2} \dots \mathfrak{p}_r^{h_r}$$

*) Diese Definition des Quotienten zweier Ideale stimmt mit der in § 4, 8. gegebenen völlig überein.

die Exponenten h_i die Reihe der Zahlen 0, 1, 2, ... e_i durchlaufen läßt (wobei unter $\mathfrak{p}^0$ das Ideal $\mathfrak{o}$ zu verstehen ist). Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Ideale

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}; \quad \mathfrak{b} = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\dots\mathfrak{p}_r^{f_r}$$

(worin die Exponenten e, f auch zum Teil Null sein können), so erhält man den größten gemeinschaftlichen Teiler und das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ in der Form

$$\mathfrak{p}_1^{g_1}\mathfrak{p}_2^{g_2}\dots\mathfrak{p}_r^{g_r},$$

wenn man für $g_1, g_2, \dots g_r$ für ersteren die kleinsten, für letzteres die größten unter den Zahlen $e_1, f_1; e_2, f_2; \dots e_r, f_r$ nimmt.

6. Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Ideale, so ist allgemein

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Beweis. Es sei, wie in 5., $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, so gibt es, weil $\mathfrak{a}_1$ ein echter Teiler von $\mathfrak{a}$ ist, in $\mathfrak{a}_1$ eine durch $\mathfrak{a}$ nicht teilbare Funktion η. Das kleinste gemeinschaftliche Vielfache und der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ sind bzw. $\mathfrak{p}_1\eta$ und $\mathfrak{a}_1$, wie sich (nach 5.) sofort aus der Zerlegung von $\mathfrak{a}$ und $\mathfrak{o}\eta$ in ihre Primfaktoren ergibt. Hieraus folgt aber nach § 8, 14.

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{a}_1).$$

Durch Wiederholung desselben Schlusses für $\mathfrak{a}_1$ usf. ergibt sich, wenn $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_r$ ist:

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)\dots N(\mathfrak{p}_r)$$

und daraus

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

7. Jedes Primideal ist ein Ideal ersten Grades (§ 7) und umgekehrt, jedes Ideal ersten Grades ist ein Primideal*).

Beweis. Ist $\mathfrak{p}$ ein Primideal, so ist $N(\mathfrak{p})$ durch $\mathfrak{p}$ teilbar, und daher wenigstens einer der Linearfaktoren von $N(\mathfrak{p})$, etwa $z - c$, durch $\mathfrak{p}$ teilbar (§ 8, 18.). Ist ω eine beliebige Funktion in $\mathfrak{o}$, welche der Gleichung genügt:

$$\omega^n + a_1\omega^{n-1} + \dots + a_{n-1}\omega + a_n = 0,$$

so erhält man daraus, indem man die ganzen rationalen Funktionen $a_1, a_2, \dots a_n$ auf ihre konstanten Reste $a_1^{(0)}, a_2^{(0)}, \dots a_n^{(0)}$ nach $z - c$ reduziert, und die ganze Funktion

$$\omega^n + a_1^{(0)}\omega^{n-1} + \dots + a_{n-1}^{(0)}\omega + a_n^{(0)}$$

*) Durch diesen Satz unterscheidet sich die Theorie der algebraischen Funktionen wesentlich von der analogen Theorie der algebraischen Zahlen.

in ihre Linearfaktoren $(\omega - b_1)$, $(\omega - b_2), \ldots (\omega - b_n)$ zerlegt:

$$(\omega - b_1)\ (\omega - b_2)\ \ldots (\omega - b_n) = (z - c)\,\omega' \equiv 0 \pmod{\mathfrak{p}}.$$

Es muß also wenigstens einer der Faktoren $\omega - b_1$, $\omega - b_2, \ldots$ durch $\mathfrak{p}$ teilbar sein, d. h. es ist

$$\omega \equiv b \pmod{\mathfrak{p}},$$

worin b eine Konstante bedeutet. Da hiernach jede Funktion in $\mathfrak{o}$ kongruent einer Konstanten ist (mod. $\mathfrak{p}$), so ist nach § 6 $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = z - c$ eine lineare Funktion von z, wodurch der erste Teil der Behauptung erwiesen ist.

Umgekehrt: ist $\mathfrak{q}$ ein Ideal ersten Grades, und

$$N(\mathfrak{q}) = z - c,$$

so ist $\mathfrak{q}$ gewiß durch ein Primideal $\mathfrak{p}$ teilbar, und da $N(\mathfrak{q})$ durch $N(\mathfrak{p})$ teilbar ist, so ist $(N(\mathfrak{p}) = N(\mathfrak{q}) = z - c$, also (§ 8, 9.)

$$\mathfrak{p} = \mathfrak{q}.$$

Es ergibt sich hieraus, daß der Grad eines Ideals gleich ist der Anzahl der Primfaktoren, in welche sich dasselbe zerlegen läßt. Ist daher

$$\mathfrak{o}(z - c) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\ldots,$$

so ist

$$e_1 + e_2 + e_3 + \cdots = n.$$

Es folgt ferner noch, daß eine ganze rationale Funktion von z dann und nur dann durch ein Primideal $\mathfrak{p}$ teilbar ist, wenn sie durch die Norm von $\mathfrak{p}$ teilbar ist.

§ 10.

Die komplementären Basen des Körpers Ω.

1. Definition. Bilden die Funktionen $\alpha_1, \alpha_2, \ldots \alpha_n$ eine Basis von Ω, und setzt man zur Abkürzung

$$S(\alpha_r\,\alpha_s) = a_{r,s} = a_{s,r},$$

$$\Delta(\alpha_1, \alpha_2, \ldots \alpha_n) = \sum \pm a_{1,1}\,a_{2,2}\ldots a_{n,n} = a \quad (\S\ 2),$$

so läßt sich, da a von Null verschieden ist, ein ganz bestimmtes Funktionensystem $\alpha_1', \alpha_2', \ldots \alpha_n'$ aus den linearen Gleichungen bestimmen

$$\alpha_r = \sum_{1,n}^{i} a_{r,i}\alpha_i', \tag{1}$$

und da

$$\Delta(\alpha_1', \alpha_2', \ldots \alpha_n') = \frac{1}{a}$$

von Null verschieden ist, so bilden die Funktionen $\alpha_1', \alpha_2', \ldots \alpha_n$ ebenfalls eine Basis von Ω. Diese soll die zu $\alpha_1, \alpha_2, \ldots \alpha_n$ **komplementäre Basis** heißen.

2. Bezeichnet man, wenn die Indizes r, s der Zahlenreihe $1, 2 \ldots n$ angehören, mit (r, s) die Zahl 1 oder 0, je nachdem r, s gleich oder verschieden sind, so ist

$$S(\alpha_r \alpha_s') = (r, s), \tag{2}$$

denn durch Auflösung der Gleichungen (1) folgt

$$\alpha_s' = \sum^{\iota} a_{\iota, s}' \alpha_\iota;$$

$$a_{r,s}' = a_{s,r}'; \sum^{\iota} a_{r,\iota} a_{s,\iota}' = (r, s),$$

hieraus:

$$\alpha_r \alpha_s' = \sum^{\iota} a_{\iota,s}' \alpha_\iota \alpha_r; \quad S(\alpha_r \alpha_s') = \sum^{\iota} a_{\iota,s}' a_{\iota,r} = (r, s).$$

Genügt umgekehrt ein Funktionensystem β_s den Bedingungen $S(\alpha_r \beta_s) = (r, s)$, so ist $\beta_s = \alpha_s'$; denn setzt man $\beta_s = \sum^{\iota} b_{\iota,s} \alpha_\iota'$, so folgt wegen (2).

$$b_{r,s} = S(\beta_s \alpha_r) = (r, s).$$

Daraus folgt unmittelbar, daß die Beziehung der α_ι zu den α_ι' eine gegenseitige ist, d. h., daß die Basis $\alpha_1, \alpha_2, \ldots \alpha_n$ komplementär ist zu $\alpha_1', \alpha_2', \ldots \alpha_n'$.

3. Ist η eine beliebige Funktion in Ω, so kann man stets setzen

$$\eta = \sum x_\iota \alpha_\iota = \sum x_\iota' \alpha_\iota',$$

und durch Anwendung von (2) folgt:

$$x_\iota = S(\eta \alpha_\iota'), \quad x' = S(\eta \alpha_\iota),$$

also

$$\eta = \sum^{\iota} \alpha_\iota S(\eta \alpha_\iota') = \sum^{\iota} \alpha_\iota' S(\eta \alpha_\iota). \tag{3}$$

4. Ist η eine beliebige von Null verschiedene Funktion in Ω, so ist

$$\frac{\alpha_1'}{\eta}, \quad \frac{\alpha_2'}{\eta}, \quad \ldots \quad \frac{\alpha_n'}{\eta}$$

die zu $\eta \alpha_1, \eta \alpha_2, \ldots \eta \alpha_n$ komplementäre Basis. Dies folgt aus 2. wegen

$$S\left(\eta \alpha_r \cdot \frac{\alpha_s'}{\eta}\right) = S(\alpha_r \alpha_s') = (r, s).$$

5. Wenn zwei Basen von Ω, $\alpha_1, \alpha_2, \ldots \alpha_n$ und $\beta_1, \beta_2, \ldots \beta_n$ durch die n Gleichungen zusammenhängen

$$\beta_s = \sum^{\iota} x_{\iota, s}\, \alpha_\iota$$

mit rationalen Koeffizienten $x_{\iota, s}$, so hängen die zu ihnen komplementären Basen zusammen durch die n Gleichungen

$$\alpha'_r = \sum^{\iota} x_{r, \iota}\, \beta'_\iota$$

(transponierte Substitution). Es ist dies eine unmittelbare Folge aus 3. wegen

$$x_{r, s} = S(\alpha'_r \beta_s).$$

6. Es ist

$$\sum^{\iota} \alpha_\iota \alpha'_\iota = 1,$$

also:

$$\sum^{\iota, \iota'} a_{\iota, \iota'}\, \alpha'_\iota \alpha'_{\iota'} = \sum^{\iota, \iota'} a'_{\iota, \iota'}\, \alpha_\iota \alpha_{\iota'} = 1.$$

Setzt man nämlich zunächst

$$\sum \alpha_\iota \alpha_{\iota'} = \sigma,$$

so folgt aus 3. (auf die Funktionen $\eta \alpha_r$ angewandt),

$$\eta \alpha_r = \sum^{\iota} \alpha_\iota S(\eta \alpha_r \alpha'_\iota),$$

mithin, nach der Definition der Spur in § 2, (5)

$$S(\eta) = \sum^{\iota} S(\eta \alpha_\iota \alpha'_\iota) = S(\sum \eta \alpha_\iota \alpha'_\iota)$$

also:

$$S(\eta \sigma) = S(\eta),$$

und daraus, wenn man in 3. einmal $\eta = \sigma$, dann $\eta = 1$ setzt:

$$\sigma = \sum^{\iota} \alpha_\iota S(\sigma \alpha'_\iota) = \sum^{\iota} \alpha_\iota S(\alpha'_\iota) = 1.$$

Wir gehen etwas genauer ein auf die Bildung der komplementären Basen in zwei besonderen Fällen:

7. Es sei $\omega_1, \omega_2, \ldots \omega_n$ eine Basis von $\mathfrak{o}$ und $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n$ die komplementäre Basis (von Ω). Es sei

$$e_{r, s} = e_{s, r} = S(\omega_r \omega_s),$$

welches ganze rationale Funktionen sind, und

$$D = \text{konst.} \sum \pm e_{1, 1}\, e_{2, 2} \ldots e_{n, n}$$

die Diskriminante von Ω; ist dann nach 2.

$$\varepsilon_r = \frac{1}{D} \sum^{\iota} \frac{\partial D}{\partial e_{\iota,r}} \omega_\iota,$$

woraus hervorgeht, daß die Funktionen $D\varepsilon_r$ zu den ganzen Funktionen gehören. Aus 6. folgt aber ferner

$$D = \sum^{\iota,\iota'} \frac{\partial D}{\partial e_{\iota,\iota'}} \omega_\iota \omega_{\iota'}$$

und hieraus

$$\varepsilon_r \varepsilon_s = \frac{1}{D^2} \sum^{\iota,\iota'} \frac{\partial D}{\partial e_{r,\iota}} \frac{\partial D}{\partial e_{s,\iota'}} \omega_\iota \omega_{\iota'}$$

$$= \frac{1}{D} \frac{\partial D}{\partial e_{r,s}} + \frac{1}{D^2} \sum^{\iota,\iota'} \left(\frac{\partial D}{\partial e_{r,\iota}} \frac{\partial D}{\partial e_{s,\iota'}} - \frac{\partial D}{\partial e_{r,s}} \frac{\partial D}{\partial e_{\iota,\iota'}} \right) \omega_\iota \omega_{\iota'}$$

und daraus nach einem bekannten Determinantensatz:

$$\varepsilon_r \varepsilon_s = \frac{1}{D} \frac{\partial D}{\partial e_{r,s}} + \frac{1}{D} \sum^{\iota,\iota'} \frac{\partial^2 D}{\partial e_{r,\iota} \partial e_{s,\iota'}} \omega_\iota \omega_{\iota'},$$

woraus das wichtige Resultat folgt, daß auch die Funktionen $D\varepsilon_r \varepsilon_s$ zu den ganzen Funktionen gehören.

8. Es sei θ eine solche Funktion in Ω, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis von Ω bilden, und es sei also

$$(4) \qquad f(\theta) = \theta^n + a_1 \theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

mit rationalen Koeffizienten a irreduktibel. Es soll die komplementäre Basis zu $1, \theta, \theta^2, \ldots \theta^{n-1}$ aufgesucht werden. Setzen wir, wenn t eine unbestimmte Konstante bedeutet,

$$\frac{f(t)}{t-\theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1} t^{n-1},$$

oder

$$(5) \qquad \begin{cases} \eta_0 &= a_{n-1} + a_{n-2}\theta + \cdots + a_1 \theta^{n-2} + \theta^{n-1}, \\ \eta_1 &= a_{n-2} + a_{n-3}\theta + \cdots + \theta^{n-2}, \\ \cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{n-2} &= a_1 + \theta, \\ \eta_{n-1} &= 1, \end{cases}$$

so bilden die Funktionen $\eta_0, \eta_1, \ldots \eta_{n-1}$ gleichfalls eine Basis von Ω, da die Determinante der Gleichungen (5) $= (-1)^{\frac{1}{2}n(n-1)}$, also von Null verschieden ist. Es läßt sich daher jede Funktion ζ in Ω in der Form darstellen

$$\zeta = y_0 \eta_0 + y_1 \eta_1 + \cdots + y_{n-1} \eta_{n-1}.$$

Die Reihe der rationalen Funktionen $y_0, y_1, \dots y_{n-1}$ setzen wir nun fort, indem wir die Funktionen $y_n, y_{n+1}, \dots$ durch die Rekursion bestimmen

$$(6) \quad a_n y_r + a_{n-1} y_{r+1} + \cdots + a_2 y_{r+n-2} + a_1 y_{r+n-1} + y_{r+n} = 0.$$

Nun ist nach (5)

$$(7) \quad \begin{cases} \theta \eta_0 & = & - a_n \eta_{n-1}, \\ \theta \eta_1 & = \eta_0 & - a_{n-1} \eta_{n-1}, \\ \theta \eta_2 & = \eta_1 & - a_{n-2} \eta_{n-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \theta \eta_{n-1} & = \eta_{n-2} - & a_1 \eta_{n-1}, \end{cases}$$

also

$$\zeta \theta = y_1 \eta_0 + y_2 \eta_1 + \cdots + y_{n-1} \eta_{n-2} + y_n \eta_{n-1},$$

und ebenso allgemein für jedes ganze positive r:

$$\zeta \theta^r = y_r \eta_0 + y_{r+1} \eta_1 + \cdots + y_{r+n-2} \eta_{n-2} + y_{r+n-1} \eta_{n-1},$$

oder, wenn man $\eta_0, \eta_1, \dots \eta_{n-1}$ durch $1, \theta, \theta^2, \dots \theta^{n-1}$ ausdrückt:

$$\zeta \theta^r = x_0^{(r)} + x_1^{(r)} \theta + x_2^{(r)} \theta^2 + \cdots + x_{n-1}^{(r)} \theta^{n-1},$$

worin

$$\begin{aligned} x_0^{(r)} &= y_r a_{n-1} + y_{r+1} a_{n-2} + \cdots + y_{r+n-2} a_1 + y_{r+n-1}, \\ x_1^{(r)} &= y_r a_{n-2} + y_{r+1} a_{n-3} + \cdots + y_{r+n-2}, \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_{n-2}^{(r)} &= y_r a_1 \quad + y_{r+1}, \\ x_{n-1}^{(r)} &= y_r. \end{aligned}$$

Mithin ist [nach der Definition von S, § 2 (5)]

$$\begin{aligned} S(\zeta) &= x_0^{(0)} + x_1^{(1)} + x_2^{(2)} + \cdots + x_{n-1}^{(n-1)} \\ &= y_0 a_{n-1} + 2 y_1 a_{n-2} + \cdots + (n-1) y_{n-2} a_1 + n y_{n-1}, \end{aligned}$$

also, auf $\zeta = \eta_r$ angewandt:

$$S(\eta_r) = (r+1) a_{n-1-r}; \quad S(\eta_{n-1-r}) = (n-r) a_r,$$

worin $a_0 = 1$ zu setzen ist.

Setzt man daher zur Abkürzung

$$S(\theta^r) = s_r,$$

so folgt, so lange $r \gtrless n$, mittels (5)

$$(8) \quad (n-r) a_r = a_r s_0 + a_{r-1} s_1 + \cdots + a_1 s_{r-1} + s_r$$

und nach (4) allgemein

$$(9) \quad 0 = a_n s_r + a_{n-1} s_{r+1} + \cdots + a_1 s_{r+n-1} + s_{r+n}.$$

Aus diesen Formeln folgt aber ferner:

$$(10)\quad \begin{cases} f'(\theta) = n\,\theta^{n-1} + (n-1)\,a_1\,\theta^{n-1} + \cdots + 2\,a_{n-2}\,\theta + a_{n-1} \\ \qquad = s_0\,\eta_0 + s_1\,\eta_1 + \cdots + s_{n-1}\,\eta_{n-1}, \\ \theta^r f'(\theta) = s_r\,\eta_0 + s_{r+1}\,\eta_1 + \cdots + s_{r+n-2}\,\eta_{n-2} + s_{r+n-1}\,\eta_{n-1}. \end{cases}$$

Beachtet man nun den Wert der Determinante des Gleichungssystems (5), so folgt hieraus mit Rücksicht auf die Definition der Norm und der Diskriminante in § 2 (4) und (12) die wichtige Formel

$$(11)\quad Nf'(\theta) = (-1)^{1/2\,n(n-1)} \begin{vmatrix} s_0, & s_1, \cdots s_{n-1} \\ s_1, & s_2, \cdots s_n \\ \cdots & \cdots \\ s_{n-1}, & s_n, \cdots s_{2n-2} \end{vmatrix} = (-1)^{1/2\,n(n-1)}\,\Delta(1, \theta, \theta^2, \ldots \theta^{n-1}).$$

Die Gleichungen (10) ergeben aber auch mit Rücksicht auf die Definition 1. die zu $1, \theta, \theta^2, \ldots \theta^{n-1}$ komplementäre Basis:

$$\frac{\eta_0}{f'(\theta)}, \quad \frac{\eta_1}{f'(\theta)}, \quad \cdots \quad \frac{\eta_{n-1}}{f'(\theta)}.$$

9. Bedeutet $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n]$ einen Modul, dessen Basis zugleich eine Basis Ω ist, so erhält man aus der zu $\alpha_1, \alpha_2, \ldots \alpha_n$ komplementären Basis von Ω, $\alpha_1', \alpha_2', \ldots \alpha_n'$ einen anderen Modul $\mathfrak{a}' = [\alpha_1', \alpha_2', \ldots \alpha_n']$, welcher der zu $\mathfrak{a}$ komplementäre Modul genannt wird. Derselbe ist, wie sich aus 5. in Verbindung mit § 4, 2. sofort ergibt, von der Wahl der Basis von $\mathfrak{a}$ unabhängig.

10. Wir betrachten insbesondere den zu $\mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n]$ komplementären Modul $\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n]$. Setzen wir

$$\omega_r\,\omega_s = \sum_{\iota}^{\iota} e_{r,s}^{(\iota)}\,\omega_\iota,$$

so ist nach 3.

$$e_{r,s}^{(\iota)} = e_{s,r}^{(\iota)} = S(\omega_r\,\omega_s\,\varepsilon_\iota)$$

eine ganze rationale Funktion von z, und es folgt:

$$\omega_r\,\varepsilon_s = \sum_{\iota}^{\iota} e_{r,\iota}^{(s)}\,\varepsilon_\iota.$$

Hieraus ergibt sich, daß der Modul $\mathfrak{o}\,\mathfrak{e}$ (§ 4, 7.) teilbar ist durch $\mathfrak{e}$; andererseits ist, weil $\mathfrak{o}$ die Funktion 1 enthält, $\mathfrak{e}$ teilbar durch $\mathfrak{o}\,\mathfrak{e}$, also

$$\mathfrak{o}\,\mathfrak{e} = \mathfrak{e},$$

d. h. der Modul $\mathfrak{e}$, der zwar nicht bloß ganze Funktionen enthält, besitzt die charakteristische Eigenschaft II. § 7 der Ideale. Dasselbe gilt infolgedessen auch von dem Modul $\mathfrak{e}^2$. Da die beiden Moduln

De, De^2 nach 7. nur ganze Funktionen enthalten, so sind dieselben Ideale, und aus 7. ergibt sich noch

$$N(De) = D^{n-1}.$$

11. Ist θ eine Funktion in o von der Art, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis von $\mathfrak{Q}$ bildet, so daß in der irreduktibeln Gleichung

$$f(\theta) = \theta^n + a_1\theta^{n-1} + \ldots + a_{n-1}\theta + a_n = 0$$

die Koeffizienten ganze rationale Funktionen von z sind, so kann man für $r = 0, 1, 2, \ldots n-1$ die ganzen rationalen Funktionen $k_i^{(r)}$ so bestimmen, daß

$$\theta^r = \sum_{1,n}^{i} k_i^{(r)} \omega_i$$

wird. Wendet man hierauf den Satz 5. und 8. an, so folgt:

$$f'(\theta)\varepsilon_s = k_s^{(0)}\eta_0 + k_s^{(1)}\eta_1 + \ldots + k_s^{(n-1)}\eta_{n-1},$$

und hieraus ergibt sich, daß der Modul

$$f'(\theta)\mathfrak{e} = \mathfrak{k}$$

nur ganze Funktionen enthält. Aus 10. schließt man, daß derselbe ein Ideal ist.

§ 11.

Das Verzweigungsideal.

1. Hilfssatz. Sind je zwei der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ relativ prim, so existiert immer eine Funktion, welche in bezug auf jedes von ihnen einer gegebenen Funktion in o kongruent ist.

Beweis. Man setze

$$\mathfrak{m} = \mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 = \cdots;$$

der größte gemeinschaftliche Teiler von $\mathfrak{a}_1 = \mathfrak{b}\mathfrak{c}\ldots$, $\mathfrak{b}_1 = \mathfrak{a}\mathfrak{c}\ldots$ $\mathfrak{c}_1 = \mathfrak{a}\mathfrak{b}\ldots$ ist alsdann gleich o, da kein Primideal zugleich in $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \ldots$ aufgehen kann. Folglich kann man (§ 4, 5.) α_1 aus $\mathfrak{a}_1$, β_1 aus $\mathfrak{b}_1$, γ_1 aus $\mathfrak{c}_1, \ldots$ so auswählen, daß

$$\alpha_1 + \beta_1 + \gamma_1 + \cdots = 1,$$

also:

$$\begin{aligned}
&\alpha_1 \equiv 1, \quad \beta_1 \equiv 0, \quad \gamma_1 \equiv 0, \quad \ldots \quad (\text{mod. } \mathfrak{a}),\\
&\alpha_1 \equiv 0, \quad \beta_1 \equiv 1, \quad \gamma_1 \equiv 0, \quad \ldots \quad (\text{mod. } \mathfrak{b}),\\
&\alpha_1 \equiv 0, \quad \beta_1 \equiv 0, \quad \gamma_1 \equiv 1, \quad \ldots \quad (\text{mod. } \mathfrak{c}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Sind daher $\lambda, \mu, \nu, \ldots$ gegebene Funktionen in o, so genügt

$$\omega \equiv \lambda\alpha_1 + \mu\beta_1 + \nu\gamma_1 + \cdots \pmod{\mathfrak{m}}$$

den Bedingungen

$$\omega \equiv \lambda \pmod{\mathfrak{a}}, \quad \omega \equiv \mu \pmod{\mathfrak{b}}, \quad \omega \equiv \nu \pmod{\mathfrak{c}}, \ldots$$

2. Es seien $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ die sämtlichen voneinander verschiedenen in einer beliebigen linearen Funktion $z - c$ aufgehenden Primideale und

$$o(z-c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots, \quad e + e_1 + e_2 + \cdots = n \ (\S\ 9,\ 7.).$$

Man wähle die Funktionen $\lambda, \lambda_1, \lambda_2, \ldots$ teilbar bzw. durch $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$, aber nicht durch $\mathfrak{p}^2, \mathfrak{p}_1^2, \mathfrak{p}_2^2, \ldots$ und lasse $b, b_1, b_2, \ldots$ beliebige jedoch voneinander verschiedene Konstanten bedeuten. Nach 1. läßt sich dann eine Funktion ζ bestimmen, welche den Kongruenzen genügt

$$\zeta \equiv b + \lambda \pmod{\mathfrak{p}^2}, \quad \zeta \equiv b_1 + \lambda_1 \pmod{\mathfrak{p}_1^2}, \quad \zeta \equiv b_2 + \lambda_2 \pmod{\mathfrak{p}_2^2}, \ldots,$$

also

$$\zeta \equiv b \pmod{\mathfrak{p}}, \quad \zeta \equiv b_1 \pmod{\mathfrak{p}_1}, \quad \zeta \equiv b_2 \pmod{\mathfrak{p}_2}, \ldots,$$

so daß, wenn a irgendeine Konstante bedeutet, $\zeta - a$ höchstens durch eines der Primideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ und niemals durch eines ihrer Quadrate teilbar ist. Ist daher $\varphi(t) = \Pi(t-a)$ eine ganze Funktion der Variablen t mit konstanten Koeffizienten, so ist $\varphi(\zeta) = \Pi(\zeta - a)$ stets und nur dann durch $\mathfrak{p}^m$ teilbar, wenn $\varphi(t)$ algebraisch durch $(t-b)^m$ teilbar ist, und wenn $\mathfrak{p}^m$ die höchste in $\varphi(\zeta)$ aufgehende Potenz von $\mathfrak{p}$ ist, so ist folglich $\mathfrak{p}^{m-1}$ die höchste in $\varphi'(\zeta)$ aufgehende Potenz von $\mathfrak{p}$. Soll daher $\varphi(\zeta)$ durch $z - c$ teilbar sein, so muß $\varphi(t)$ durch die Funktion n^{ten} Grades

$$\psi(t) = (t-b)^e (t-b_1)^{e_1} (t-b_2)^{e_2} \cdots$$

teilbar sein. Mithin ist die Kongruenz

$$x_0 + x_1\zeta + x_2\zeta^2 + \cdots + x_{n-1}\zeta^{n-1} \equiv 0 \pmod{z-c}$$

nur durch solche ganze rationale x zu befriedigen, die alle durch $z - c$ teilbar sind. Setzt man also, indem man mit $k_1^{(0)}, k_1^{(1)}, \ldots$ ganze rationale Funktionen von z und mit $\omega_1, \omega_2, \ldots \omega_n$ eine Basis von o bezeichnet:

$$\begin{aligned}
1 &= k_1^{(0)}\omega_1 + k_2^{(0)}\omega_2 + \cdots + k_n^{(0)}\omega_n, \\
\zeta &= k_1^{(1)}\omega_1 + k_2^{(1)}\omega_2 + \cdots + k_n^{(1)}\omega_n, \\
\zeta^2 &= k_1^{(2)}\omega_1 + k_2^{(2)}\omega_2 + \cdots + k_n^{(2)}\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\zeta^{n-1} &= k_1^{(n-1)}\omega_1 + k_2^{(n-1)}\omega_2 + \cdots + k_n^{(n-1)}\omega_n,
\end{aligned}$$

so kann die Determinante

$$k = \sum \pm k_1^{(0)} k_2^{(1)} \cdots k_n^{(n-1)}$$

weder identisch verschwinden, noch durch $z - c$ teilbar sein (vgl. die Note zu § 9, 1.).

Es folgt also, daß

$$N(t - \zeta) = f(t, z)$$

irreduktibel ist. Da nun $f(\zeta, z) = 0$, also $f(\zeta, c)$ durch $z - c$ teilbar ist, so muß $f(t, c)$ durch $\psi(t)$ teilbar, also, da beide Funktionen von gleichem Grade sind,

$$f(t, c) = \psi(t)$$

sein, woraus man noch für eine folgende Anwendung schließt:

$$S(\zeta) \equiv e b + e_1 b_1 + e_2 b_2 + \cdots \pmod{z - c},$$

und, indem man dieselbe Betrachtung auf die Funktionen $\zeta^2, \zeta^3 \ldots$ anwendet, was, falls keine der Konstanten b verschwindet, sicher gestattet ist:

$$S(\zeta^2) \equiv e b^2 + e_1 b_1^2 + e_2 b_2^2 + \cdots \pmod{z - c},$$
$$S(\zeta^3) \equiv e b^3 + e_1 b_1^3 + e_2 b_2^3 + \cdots \pmod{z - c}.$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Es ist also $\mathfrak{p}^e$ die höchste in $f(\zeta, c)$, also $\mathfrak{p}^{e-1}$ die höchste in $f'(\zeta, c)$ aufgehende Potenz von $\mathfrak{p}$, und da

$$f'(\zeta, c) \equiv f'(\zeta, z) \pmod{\mathfrak{p}^e},$$

so ist $\mathfrak{p}^{e-1}$ auch die höchste in $f'(\zeta, z)$ aufgehende Potenz von $\mathfrak{p}$. Hieraus ergibt sich

$$\circ f'(\zeta, z) = \mathfrak{m}\, \mathfrak{p}^{e-1} \mathfrak{p}_1^{e_1-1} \ldots,$$

worin $\mathfrak{m}$ und folglich auch $N(\mathfrak{m})$ relativ prim zu $z - c$ ist.

Ist nun D die Diskriminante von Ω, so ist hiernach und nach § 10, (11) und § 2, (13) (von konstanten Faktoren abgesehen)

$$N f'(\zeta, z) = \Delta(1, \zeta, \zeta^2, \ldots \zeta^{n-1}) = D k^2 = (z - c)^{n-s} N(\mathfrak{m}),$$

wenn s die Anzahl der verschiedenen in $z - c$ aufgehenden Primideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ bedeutet; und da k und $N(\mathfrak{m})$ durch $z - c$ nicht teilbar sind, so ist $(z - c)^{n-s}$ die höchste in D aufgehende Potenz von $z - c$. Folglich:

$$D = \Pi(z - c)^{n-s}, \tag{1}$$

worin das Produktzeichen Π sich auf alle solche linearen Ausdrücke $z - c$ bezieht, in denen weniger als n verschiedene Primfaktoren

aufgehen, die also durch die zweite oder eine höhere Potenz eines Primideals teilbar sind.

Es gibt also nur eine endliche Anzahl linearer Funktionen $z - c$, die durch das Quadrat eines Primideals teilbar sind.

Wir setzen nun

$$\mathfrak{z} = \Pi \mathfrak{p}^{e-1}, \tag{2}$$

worin sich das Produktzeichen Π auf alle diejenigen Primideale $\mathfrak{p}$ bezieht, von denen eine höhere als die erste, nämlich die e^{te} Potenz in ihrer Norm aufgeht, und nennen dieses Ideal $\mathfrak{z}$ das Verzweigungsideal. Aus (1) und (2) folgt sofort

$$N(\mathfrak{z}) = D. \tag{3}$$

Da ferner $n - s \geqq e - 1$, also $e(n-s) - 2(e-1) \geqq (e-1)(e-2) \geqq 0$ ist, so ist D teilbar durch $\mathfrak{p}^{2(e-1)}$, also auch durch $\mathfrak{z}^2$, und man kann, wenn man mit $\mathfrak{d}$ gleichfalls ein Ideal bezeichnet, setzen:

$$\mathfrak{o} D = \mathfrak{d} \mathfrak{z}^2, \quad N(\mathfrak{d}) = D^{n-2}. \tag{4}$$

3. Ist eine Funktion ϱ in $\mathfrak{o}$ durch jedes in $z - c$ aufgehende Primideal teilbar, so ist $S(\varrho)$ durch $z - c$ teilbar.

Beweis. Es sei ζ dieselbe Funktion wie in 2., so daß man setzen kann:

$$x\varrho = x_0 + x_1 \zeta + x_2 \zeta^2 + \cdots + x_{n-1} \zeta^{n-1},$$

worin die Koeffizienten x, x_0, x_1, $\ldots$ x_{n-1} ganze rationale Funktionen von z ohne gemeinsamen Teiler sind, von denen die erste durch $z - c$ nicht teilbar ist (vgl. 2.). Aus unserer Voraussetzung über die Funktion ϱ folgt, wenn die Konstanten b dieselbe Bedeutung wie in 2. haben,

$$\begin{aligned}
&x_0 + x_1 b + x_2 b^2 + \cdots + x_{n-1} b^{n-1} \equiv 0 \pmod{z - c},\\
&x_0 + x_1 b_1 + x_2 b_1^2 + \cdots + x_{n-1} b_1^{n-1} \equiv 0 \pmod{z - c},\\
&x_0 + x_1 b_2 + x_2 b_2^2 + \cdots + x_{n-1} b_2^{n-1} \equiv 0 \pmod{z - c},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

und hieraus, indem man die Kongruenzen mit e, e_1, e_2, $\ldots$ multipliziert und addiert:

$$x_0 n + x_1 S(\zeta) + x_2 S(\zeta^2) + \cdots + x_{n-1} S(\zeta^{n-1}) = x S(\varrho) \equiv 0 \pmod{z - c},$$

also, da x durch $z - c$ nicht teilbar ist,

$$S(\varrho) \equiv 0 \pmod{(z-c)}$$

w. z. b. w.

4. Es sei jetzt

$$r = (z-c)\,(z-c_1)\,(z-c_2)\ldots$$

das Produkt sämtlicher voneinander verschiedenen Linearfaktoren von D und

$$\mathfrak{r} = \mathfrak{p}\,\mathfrak{p}_1\,\mathfrak{p}_2\ldots$$

das Produkt der sämtlichen voneinander verschiedenen in r aufgehenden Primideale. Ist wie oben $\mathfrak{z}$ das Verzweigungsideal, so ist

$$\mathfrak{r}\mathfrak{z} = \Pi\mathfrak{p}^e = \mathfrak{o}\,r \tag{5}$$

und mithin

$$N(\mathfrak{r}) = \frac{r^n}{D}.$$

Jede Funktion ϱ in $\mathfrak{r}$ hat nach 3. die Eigenschaft, daß $S(\varrho)$ durch r teilbar ist. Ist nun, wie in § 10

$$\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n]$$

der zu $\mathfrak{o}$ komplementäre Modul, ϱ eine beliebige Funktion in $\mathfrak{r}$, so kann man setzen

$$\varrho = x_1\varepsilon_1 + x_2\varepsilon_2 + \cdots + x_n\varepsilon_n,$$

worin nach § 10, 3.

$$x_i = S(\varrho\,\omega_i),$$

also, da $\varrho\,\omega_i$ eine Funktion in $\mathfrak{r}$ ist, x_i eine durch r teilbare ganze rationale Funktion von z. Hieraus folgt, daß das Ideal $\mathfrak{r}$ durch den Modul $r\mathfrak{e}$ teilbar ist. Es ist also auch das Ideal $D\mathfrak{r}$ teilbar durch das Ideal $rD\mathfrak{e}$. Zugleich ist

$$N(D\mathfrak{r}) = r^n D^{n-1}, \quad N(rD\mathfrak{e}) = r^n D^{n-1} \quad (\S\ 10,\ 10.);$$

mithin nach § 8, 9.

$$D\mathfrak{r} = rD\mathfrak{e}$$

oder

$$\mathfrak{r} = r\mathfrak{e}. \tag{6}$$

Woraus mittels der obigen Bemerkung über ϱ folgt, daß, wenn ε eine beliebige Funktion in $\mathfrak{e}$ bedeutet, $S(\varepsilon)$ eine ganze rationale Funktion von z ist. Aus der Formel (6) folgt durch Multiplikation mit $\mathfrak{z}$ nach (5)

$$\mathfrak{r}\mathfrak{z} = r\mathfrak{e}\mathfrak{z} = \mathfrak{o}\,r$$

und folglich

$$\mathfrak{e}\mathfrak{z} = \mathfrak{o}. \tag{7}$$

Multipliziert man die letzte Gleichung mit D, so ergibt sich aus (4)

$$\mathfrak{e}\, D\, \mathfrak{z} = \mathfrak{z}^2\, \mathfrak{d},$$

folglich

$$D\, \mathfrak{e} = \mathfrak{z}\, \mathfrak{d} \tag{8}$$

und durch Multiplikation dieser Gleichung mit $\mathfrak{e}$ nach (7)

$$D\, \mathfrak{e}^2 = \mathfrak{d}. \tag{9}$$

5. Ist θ eine ganze Funktion von z in Ω und $N(t-\theta) = f(t)$, so ist $f'(\theta)$ teilbar durch das Verzweigungsideal $\mathfrak{z}$.

Beweis. Ist $f(t)$ reduktibel, so ist $f'(\theta) = 0$, also sicher teilbar durch $\mathfrak{z}$. Im anderen Fall ist nach § 10, 11.

$$\mathfrak{e}\, f'(\theta) = \mathfrak{k}$$

ein Ideal, folglich durch Multiplikation mit $\mathfrak{z}$ nach (7)

$$\mathfrak{o}\, f'(\theta) = \mathfrak{k}\, \mathfrak{z}. \tag{10}$$

Zugleich folgt, wenn wir wie in § 10, 11.

$$\theta^r = \sum^{\iota} k_{\iota}^{(r)}\, \omega_{\iota},$$

$$k = \sum \pm k_1^{(0)}\, k_2^{(1)} \dots k_n^{(n-1)}$$

setzen,

$$N f'(\theta) = N(\mathfrak{k})\, N(\mathfrak{z}) = D\, N(\mathfrak{k})$$
$$= \text{konst.}\ k^2 D \quad [\S\ 10, (11) \text{ und } \S\ 2, (13)],$$

also:

$$N(\mathfrak{k}) = \text{konst.}\ k^2 \tag{11}$$

ein vollständiges Quadrat.

§ 12.

Die gebrochenen Funktionen von z im Körper Ω.

1. Jede beliebige Funktion η in Ω läßt sich nach § 3, 3. auf unendlich viele Arten als Quotient zweier ganzen Funktionen von z darstellen (der Nenner kann sogar eine ganze rationale Funktion von z sein). Es sei also

$$\eta = \frac{\nu}{\mu}$$

und μ, ν ganze Funktionen von z (Funktionen in $\mathfrak{o}$). Ist nun $\mathfrak{m}$ der größte gemeinschaftliche Teiler der beiden Hauptideale $\mathfrak{o}\mu$, $\mathfrak{o}\nu$, also, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind,

$$\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}, \quad \mathfrak{o}\nu = \mathfrak{b}\mathfrak{m}, \tag{1}$$

so folgt (§ 4, 6.)

$$\mathfrak{a}\nu = \mathfrak{b}\mu \quad \text{oder} \quad \mathfrak{a}\eta = \mathfrak{b}. \tag{2}$$

Ist also α eine beliebige Funktion in $\mathfrak{a}$, so ist $\alpha\eta$ in $\mathfrak{b}$ enthalten, also jedenfalls eine ganze Funktion von z. Ist umgekehrt α eine ganze Funktion von z, welche die Eigenschaft hat, daß $\alpha\eta = \beta$ eine ganze Funktion ist, so folgt

$$\alpha\nu = \beta\mu,$$

also nach (1)

$$\alpha\mathfrak{b} = \beta\mathfrak{a};$$

da nun $\mathfrak{a}$, $\mathfrak{b}$ relativ prim sind, so muß α durch $\mathfrak{a}$, β durch $\mathfrak{b}$ teilbar sein, und daraus folgt:

Es ist $\mathfrak{a}$ der Inbegriff aller derjenigen ganzen Funktionen α, welche die Eigenschaft haben, daß $\alpha\eta$ eine ganze Funktion ist, und der Inbegriff aller dieser ganzen Funktionen $\alpha\eta$ ist das Ideal $\mathfrak{b}$; oder anders ausgedrückt:

Es ist $\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\eta$ und $\mathfrak{o}$, ebenso $\mathfrak{a}$ das kleinste gemeinschaftliche Vielfache von $\frac{\mathfrak{o}}{\eta}$ und $\mathfrak{o}$. Hiernach muß, wenn $\mathfrak{a}'$, $\mathfrak{b}'$ zwei der Bedingung

$$\mathfrak{a}'\eta = \mathfrak{b}'$$

genügende Ideale sind, $\mathfrak{a}'$ durch $\mathfrak{a}$ teilbar sein. Sei also

$$\mathfrak{a}' = \mathfrak{n}\mathfrak{a},$$

so folgt:

$$\mathfrak{b}' = \mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

Umgekehrt ist auch für ein beliebiges Ideal $\mathfrak{n}$

$$\mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

2. Es seien jetzt $\mathfrak{a}$, $\mathfrak{b}$ zwei der Bedingung

$$\mathfrak{a}\eta = \mathfrak{b}$$

genügende Ideale, gleichviel ob relativ prim oder nicht. Der Quotient $\frac{\mathfrak{b}}{\mathfrak{a}}$ ist nach § 4, 8. der Inbegriff aller derjenigen Funktionen γ, welche die Eigenschaft haben, daß $\mathfrak{a}\gamma$ durch $\mathfrak{b}$ teilbar ist. Zu diesen Funktionen gehören gewiß alle Funktionen von der Form $\omega\eta$, wenn ω eine beliebige Funktion in $\mathfrak{o}$ bedeutet. Aber auch umgekehrt ist jede Funktion γ von dieser Form; denn da $\mathfrak{a}\gamma$ durch $\mathfrak{b}$, also auch durch $\mathfrak{o}$ teilbar ist, so ist es ein Ideal (da es die Eigenschaften I., II., § 7 besitzt), also wenn $\mathfrak{c}$ gleichfalls ein Ideal ist:

$$\mathfrak{a}\gamma = \mathfrak{c}\mathfrak{b}$$

und durch Multiplikation mit η

$$\mathfrak{b}\gamma = \mathfrak{c}\mathfrak{b}\eta.$$

Ist nun wie oben $\eta = \frac{\nu}{\mu}$, und, wenn ϱ, σ ganze Funktionen sind, $\gamma = \frac{\varrho}{\sigma}$, so folgt hieraus

$$\mathfrak{b}\,\varrho\,\mu = \mathfrak{c}\,\mathfrak{b}\,\nu\,\sigma,$$

also:

$$\mathfrak{o}\,\varrho\,\mu = \mathfrak{c}\,\nu\,\sigma, \quad \mathfrak{o}\,\gamma = \mathfrak{c}\,\eta.$$

Beides zusammen liefert den Satz

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}. \tag{3}$$

Sind in dieser Darstellung $\mathfrak{b}$, $\mathfrak{a}$ relativ prim, was nach 1. stets und nur auf eine Weise angenommen werden kann, so soll $\mathfrak{b}$ das **Oberideal**, $\mathfrak{a}$ das **Unterideal** der Funktion η heißen.

3. Ist wieder allgemein

$$\mathfrak{a}\,\eta = \mathfrak{b}, \quad \text{also} \quad \mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

und α eine beliebige Funktion in $\mathfrak{a}$, β eine zugehörige Funktion in $\mathfrak{b}$, so ist

$$\eta = \frac{\beta}{\alpha} \text{ und } \mathfrak{a}\,\beta = \mathfrak{b}\,\alpha.$$

Hieraus folgt durch Bildung der Normen

$$N(\eta) = \text{konst.}\,\frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

4. Sind η, η' zwei Funktionen in Ω und ist wie in 1.

$$\mathfrak{a}\,\eta = \mathfrak{b}; \quad \mathfrak{a}'\,\eta' = \mathfrak{b}',$$

gleichviel ob $\mathfrak{a}$, $\mathfrak{b}$; $\mathfrak{a}'$, $\mathfrak{b}'$ relativ prim sind oder nicht, so folgt

$$\mathfrak{a}\,\mathfrak{a}'\,\eta\,\eta' = \mathfrak{b}\,\mathfrak{b}'.$$

Es folgen also aus

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\,\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}'}$$

die Gleichungen

$$\mathfrak{o}\,\eta\,\eta' = \frac{\mathfrak{b}\,\mathfrak{b}'}{\mathfrak{a}\,\mathfrak{a}'}, \quad \mathfrak{o}\,\frac{1}{\eta} = \frac{\mathfrak{a}}{\mathfrak{b}}, \quad \mathfrak{o}\,\frac{\eta}{\eta'} = \frac{\mathfrak{b}\,\mathfrak{a}'}{\mathfrak{a}\,\mathfrak{b}'}.$$

5. Ist $\mathfrak{a}\,\eta = \mathfrak{b}$, $\mathfrak{a}\,\eta' = \mathfrak{b}'$, so wird auch

$$\mathfrak{a}\,(\eta \pm \eta') = \mathfrak{b}''$$

ein Ideal sein, weil, wenn $\alpha\,\eta$, $\alpha\,\eta'$ ganze Funktionen sind, stets auch $\alpha\,(\eta \pm \eta')$ eine solche ist. Ist also

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\,\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}},$$

so folgt

$$\mathfrak{o}\,(\eta \pm \eta') = \frac{\mathfrak{b}''}{\mathfrak{a}};$$

haben die beiden Ideale $\mathfrak{b}$, $\mathfrak{b}'$ einen gemeinsamen Teiler, so ist derselbe auch Teiler von $\mathfrak{b}''$.

6. Es sei jetzt ϱ eine Funktion in Ω, deren Oberideal durch ein beliebig gegebenes Primideal $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist (solche Funktionen existieren stets; dieselben können sogar ganze Funktionen von z sein), also

$$\mathfrak{o}\,\varrho = \frac{\mathfrak{m}\,\mathfrak{p}}{\mathfrak{n}},$$

worin $\mathfrak{m}$, $\mathfrak{n}$ durch $\mathfrak{p}$ nicht teilbare Ideale sind. Sei ferner η eine beliebige Funktion in Ω, deren Unterideal durch $\mathfrak{p}$ nicht teilbar ist, also

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

und $\mathfrak{a}$ nicht teilbar durch $\mathfrak{p}$. Man wähle eine beliebige Funktion α in $\mathfrak{a}$, die nicht durch $\mathfrak{p}$ teilbar ist, und eine entsprechende Funktion β in $\mathfrak{b}$, so daß

$$\eta = \frac{\beta}{\alpha}$$

wird. Sei

$$\alpha \equiv \alpha_0, \quad \beta \equiv \beta_0 \pmod{\mathfrak{p}}, \quad c_0 = \frac{\beta_0}{\alpha_0},$$

worin α_0, β_0, c_0 Konstanten sind, deren erste von Null verschieden ist. Nach 5. ist

$$\mathfrak{o}(\eta - c_0) = \mathfrak{o}\frac{\beta - c_0\alpha}{\alpha} = \frac{\mathfrak{b}_1}{\mathfrak{a}},$$

und aus

$$\mathfrak{a}(\beta - c_0\alpha) = \mathfrak{b}_1\alpha, \quad \beta - c_0\alpha \equiv 0 \pmod{\mathfrak{p}}$$

folgt, da α durch $\mathfrak{p}$ nicht teilbar ist, daß $\mathfrak{b}_1$ durch $\mathfrak{p}$ teilbar sein muß. Setzt man also

$$\eta - c_0 = \varrho\,\eta_1,$$

so ist auch das Unterideal von η_1 durch $\mathfrak{p}$ nicht teilbar. Auf diese Weise läßt sich eine ganz bestimmte Reihe von Konstanten $c_0, c_1, \ldots c_{r-1}, \ldots$ derart ermitteln, daß

$$\begin{aligned}
\eta &= c_0 + \varrho\,\eta_1,\\
\eta_1 &= c_1 + \varrho\,\eta_2,\\
&\cdots\cdots\cdots\cdots\\
\eta_{r-1} &= c_{r-1} + \varrho\,\eta_r, \ \ldots,
\end{aligned}$$

worin die $\eta_1, \eta_2, \ldots \eta_r, \ldots$ Funktionen bedeuten, deren Unterideale keine anderen Primfaktoren haben können als das Unterideal von η

und das Oberideal von ϱ mit Ausschluß von $\mathfrak{p}$. Demnach ist für jedes ganze positive r

$$\eta = c_0 + c_1 \varrho + \cdots + c_{r-1} \varrho^{r-1} + \eta_r \varrho^r.$$

Ist das Unterideal von ζ durch $\mathfrak{p}^s$, nicht durch $\mathfrak{p}^{s+1}$ teilbar, so kann man dieselbe Betrachtung auf die Funktion $\eta = \zeta \varrho^s$ anwenden und erhält

$$\zeta = c_0 \varrho^{-s} + c_1 \varrho^{-s+1} + \cdots + c_{r-1} \varrho^{-s+r} + \eta_r \varrho^{-s+r}.$$

§ 13.

Die rationalen Transformationen der Funktionen des Körpers Ω.

Ist z_1 eine beliebige, nicht konstante, Funktion der Körpers Ω (eine Variable in Ω), so besteht, wie in § 2 nachgewiesen, zwischen z_1 und z eine irreduktible algebraische Gleichung, welche, von Nennern befreit, in bezug auf z_1 vom Grade e, in bezug auf z vom Grade e_1 sei. Es ist, wie eben dort gezeigt, e ein Divisor von n, $n = ef$. Es sei diese Gleichung

$$G(z_1^e, z^{e_1}) = 0. \tag{1}$$

Jede rationale Funktion ζ von z und z_1 läßt sich (§ 1) mit Hilfe dieser Gleichung auf die beiden Formen bringen

$$\begin{cases} \zeta = x_0 + x_1 z_1 + \cdots + x_{e-1} z_1^{e-1}, \\ \zeta = x_0^{(1)} + x_1^{(1)} z + \cdots + x_{e_1-1}^{(1)} z^{e_1-1}, \end{cases} \tag{2}$$

und zwar nur auf eine Weise so, daß $x_0, x_1, \ldots x_{e-1}$ rationale Funktionen von z, $x_0^{(1)}, x_1^{(1)}, \ldots x_{e_1-1}^{(1)}$ rationale Funktionen von z_1 sind.

Ist nun θ eine solche Funktion, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis*) von Ω (in bezug auf z) bilden, so bilden nach § 2 die n Funktionen

$$\begin{cases} 1, & z_1, & z_1^2, \ldots & z_1^{e-1}, \\ \theta, & \theta z_1, & \theta z_1^2, \ldots & \theta z_1^{e-1}, \\ \ldots\ldots\ldots\

gleichfalls eine solche Basis, und daraus ergibt sich nach (2), daß zwischen den $e_1 f = n_1$ Funktionen

$$(4)\qquad \begin{cases} 1, & z, & z^2, \ldots & z^{e_1-1}, \\ \theta, & \theta z, & \theta z^2, \ldots & \theta z^{e_1-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta^{f-1}, & \theta^{f-1} z, & \theta^{f-1} z^2, \ldots & \theta^{f-1} z^{e_1-1}, \end{cases}$$

die zur Abkürzung mit

$$\eta_1^{(1)},\quad \eta_2^{(1)},\quad \ldots\quad \eta_{n_1}^{(1)}$$

bezeichnet sein mögen, eine Gleichung von der Form

$$x_1^{(1)}\eta_1^{(1)} + x_2^{(1)}\eta_2^{(1)} + \cdots + x_{n_1}^{(1)}\eta_{n_1}^{(1)} = 0$$

nur dann besteht, wenn die rationalen Funktionen $x_1^{(1)}, x_2^{(1)}, \ldots x_{n_1}^{(1)}$ von z_1 sämtlich verschwinden. Daraus folgt nach (2), daß jede Funktion η in Ω, und zwar nur auf eine einzige Art, darstellbar ist in der Form:

$$\eta = x_1^{(1)}\eta_1^{(1)} + x_2^{(1)}\eta_2^{(1)} + \cdots + x_{n_1}^{(1)}\eta_{n_1}^{(1)},$$

worin die $x^{(1)}$ rationale Funktionen von z_1 sind.

Jede solche Funktion η genügt einer algebraischen Gleichung vom Grade n_1, deren Koeffizienten rational von z_1 abhängen, denn es ist

$$\begin{aligned} \eta\,\eta_1^{(1)} &= x_{1,1}^{(1)}\eta_1^{(1)} + x_{1,2}^{(1)}\eta_2^{(1)} + \cdots + x_{1,n_1}^{(1)}\eta_{n_1}^{(1)}, \\ \eta\,\eta_2^{(1)} &= x_{2,1}^{(1)}\eta_1^{(1)} + x_{2,2}^{(1)}\eta_2^{(1)} + \cdots + x_{2,n_1}^{(1)}\eta_{n_1}^{(1)}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta\,\eta_{n_1}^{(1)} &= x_{n_1,1}^{(1)}\eta_1^{(1)} + x_{n_1,2}^{(1)}\eta_2^{(1)} + \cdots + x_{n_1,n_1}^{(1)}\eta_{n_1}^{(1)}, \end{aligned}$$

und mithin

$$\begin{vmatrix} x_{1,1}^{(1)} - \eta, & x_{1,2}^{(1)}, & \cdots & x_{1,n_1}^{(1)} \\ x_{2,1}^{(1)}, & x_{2,2}^{(1)} - \eta, & \cdots & x_{2,n_1}^{(1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n_1,1}^{(1)}, & x_{n_1,2}^{(1)}, & \cdots & x_{n_1,n_1}^{(1)} - \eta \end{vmatrix} = 0.$$

Es läßt sich nun zeigen, daß man eine Funktion $\eta = \theta_1$ so auswählen kann, daß θ_1 nicht zugleich einer Gleichung niedrigeren Grades, deren Koeffizienten rational von z_1 abhängen, genügt.

Wir stützen uns zum Beweis dieser Behauptung auf den folgenden Satz, dessen Beweis sich leicht durch den Schluß von $m - 1$ auf m ergibt. Ist

$$F(x_1, x_2, \ldots x_m)$$

eine ganze rationale Funktion von $x_1, x_2, \dots x_m$, deren Koeffizienten Funktionen in Ω sind, die nicht alle verschwinden, so kann man für die $x_1, x_2, \dots x_m$ solche konstanten oder rational von z_1 abhängigen Größen setzen, daß F in eine nicht verschwindende Funktion in Ω übergeht. Ist also $F(x_1, x_2, \dots x_m)$ für alle solche $x_1, x_2, \dots x_m$ gleich Null, so folgt auch für beliebige konstante oder rational von z_1 abhängige $dx_1, dx_2, \dots dx_m$

$$dF = F'(x_1)\,dx_1 + F'(x_2)\,dx_2 + \cdots + F'(x_m)\,dx_m = 0.$$

Ist nun

$$\theta_1 = x_1\,\eta_1^{(1)} + x_2\,\eta_2^{(1)} + \cdots + x_{n_1}\,\eta_{n_1}^{(1)}$$

und

$$(5)\qquad \begin{cases} 1 = x_{1,0}\,\eta_1^{(1)} + x_{2,0}\,\eta_2^{(1)} + \cdots + x_{n_1,0}\,\eta_{n_1}^{(1)}, \\ \theta_1 = x_{1,1}\,\eta_1^{(1)} + x_{2,1}\,\eta_2^{(1)} + \cdots + x_{n_1,1}\,\eta_{n_1}^{(1)}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \theta_1^m = x_{1,m}\,\eta_1^{(1)} + x_{2,m}\,\eta_2^{(1)} + \cdots + x_{n_1,m}\,\eta_{n_1}^{(1)}, \end{cases}$$

so sind die $x_{k,h}$ ganze rationale und homogene Funktionen vom Grade h von $x_1, x_2, \dots x_{n_1}$ und hängen außerdem rational von z_1 ab.

Ist also

$$\varphi(\theta_1) = a_m\,\theta_1^m + a_{m-1}\,\theta_1^{m-1} + \cdots + a_1\,\theta_1 + a_0 = 0$$

die Gleichung niedrigsten Grades, welcher θ_1 genügt, deren Koeffizienten rational von z_1 abhängen, so genügen die Funktionen $a_0, a_1, \dots a_m$ der Bedingung

$$a_0\,x_{\iota,0} + a_1\,x_{\iota,1} + \cdots + a_m\,x_{\iota,m} = 0, \qquad (\iota = 1, 2, \dots n_1)$$

und zugleich ist $m \gtreqless n_1$. Da nun nicht alle aus den Koeffizienten $x_{h,k}$ zu bildenden m-reihigen Determinanten verschwinden können, weil sonst θ_1 einer Gleichung von niedrigerem als dem m^{ten} Grade genügen würde, so folgt aus letzteren Gleichungen, daß man die $a_0, a_1, \dots a_m$ als ganze homogene Funktionen von $x_1, x_2, \dots x_{n_1}$ voraussetzen kann.

Wenn nun die Gleichung $\varphi(\theta_1) = 0$ für alle rational von z_1 abhängigen $x_1, x_2, \dots x_{n_1}$ bestehen soll, so muß nach obigem Satze auch

$$d\varphi = \varphi'(\theta_1)\,d\theta_1 + da_m\,\theta_1^m + \cdots + da_1\,\theta_1 + da_0 = 0$$

sein, und wenn $m < n_1$ ist, so lassen sich die $dx_1, dx_2, \dots dx_{n_1}$, ohne daß sie alle verschwinden, so bestimmen, daß

$$da_m : da_{m-1} : \cdots : da_1 : da_0 = a_m : a_{m-1} : \cdots : a_1 : a_0$$

und folglich

$$\varphi'(\theta_1)\, d\theta_1 = 0$$

ist. Da aber $\varphi'(\theta_1)$ vom Grade $m-1$ ist, so muß $d\theta_1 = 0$, also $dx_1 = 0$, $dx_2 = 0$, $\dots$ $dx_{n_1} = 0$ sein. Daher kann nur $m = n_1$ sein.

Ist also θ_1 so bestimmt, daß die Gleichung niedrigsten Grades

$$F_1(\theta_1, z_1) = 0$$

den Grad n_1 wirklich erreicht, so lassen sich alle Funktionen in Ω, und zwar nur auf eine Weise in der Form darstellen

$$\eta = x_0^{(1)} + x_1^{(1)}\theta_1 + \cdots + x_{n_1-1}^{(1)}\theta_1^{n_1-1},$$

worin die Koeffizienten $x_0^{(1)}, x_1^{(1)}, \dots x_{n_1-1}^{(1)}$ rational von z_1 abhängen; denn man kann unter dieser Voraussetzung $\eta_1^{(1)}, \eta_2^{(1)}, \dots \eta_{n_1}^{(1)}$ vermittelst der Gleichungen (5) in der angegebenen Weise darstellen.

Es lassen sich also sowohl z_1, θ_1 rational durch z, θ, als auch umgekehrt z, θ rational durch z_1, θ_1 darstellen.

Die Variable z, die wir bisher als die unabhängige bezeichnet haben, kann daher jede beliebige (nicht konstante) Funktion des Körpers Ω sein. Während aber die Gesamtheit aller Funktionen des Körpers Ω gänzlich ungeändert bleibt, sind die Begriffe: Basis, Norm, Spur, Diskriminante, ganze Funktion, Modul, Ideal wesentlich abhängig von der Wahl der unabhängigen Veränderlichen z.

In dem besonderen Falle nur, wenn zwei Variable z, z_1 linear voneinander abhängen, ist eine Basis von Ω in bezug auf z zugleich eine solche in bezug auf z_1; ebenso sind Normen, Spuren und Diskriminanten in diesem Falle für z und z_1 identisch.

Sind α, β irgend zwei Funktionen in Ω, so bestehen zwischen denselben Gleichungen, deren linker Teil eine ganze rationale Funktion von α und β ist.

Unter diesen ist eine (nach § 1)

$$F(\alpha, \beta) = 0,$$

welche sowohl in bezug auf α als in bezug auf β von möglichst niedrigem Grade ist, und diese soll die zwischen α und β bestehende irreduktible Gleichung heißen. Diese ist, von einem konstanten Faktor abgesehen, völlig bestimmt.

II. Abteilung.

§ 14.

Die Punkte der Riemannschen Fläche.

Die bisherigen Betrachtungen über die Funktionen des Körpers Ω waren rein formaler Natur. Alle Resultate waren rationale, d. h. nach den Regeln der Buchstabenrechnung mittels der vier Spezies abgeleitete Folgerungen aus der zwischen zwei Funktionen in Ω bestehenden irreduktiblen Gleichung. Die numerischen Werte dieser Funktionen kamen nirgends in Betracht. Man würde sogar, ohne andere Prinzipien anzuwenden, die formelle Behandlung noch wesentlich weitertreiben können, indem man zwei Funktionen des Körpers Ω nicht als durch eine Gleichung verbunden, sondern als unabhängige Veränderliche auffaßt, wobei dann alles auf algebraische Teilbarkeit von rationalen Funktionen zweier Veränderlichen hinausläuft. Wir haben auch diesen Weg durchgeführt, der jedoch in Darstellung und Ausdrucksweise sehr schwerfällig ist und bezüglich der Strenge nicht mehr leistet als der im vorhergehenden benutzte Gang. Nachdem nun aber der formale Teil der Untersuchung soweit geführt ist, drängt sich die Frage auf, in welchem Umfange es möglich ist, den Funktionen in Ω solche bestimmten Zahlenwerte beizulegen, daß alle zwischen diesen Funktionen bestehenden rationalen Relationen (Identitäten) in richtige Zahlengleichungen übergehen. Es erweist sich bei dieser Untersuchung als zweckmäßig, auch das Unendlichgroße als eine bestimmte Zahl ∞ (Konstante) zu betrachten, mit welcher nach bestimmten Regeln gerechnet wird*). Die mittels der rationalen Operationen in dem so erweiterten Zahlengebiet ausgeführten Rechnungen führen stets zu einem ganz bestimmten Zahlenresultat, wenn nicht im Verlaufe der Rechnung eines der Zeichen $\infty \pm \infty$, $0 \cdot \infty$, $\frac{0}{0}$, $\frac{\infty}{\infty}$ auftritt, Zeichen, welchen kein bestimmter Wert zukommt. Das Auftreten einer solchen Unbestimmtheit in einer Gleichung ist nicht als ein Widerspruch aufzufassen, da in diesem Falle die Gleichung gar keine bestimmte Be-

*) Das Unendliche als einen bestimmten Wert zu betrachten ist in der Funktionentheorie vielfach üblich und nützlich. Es spricht sich dies bei Riemann z. B. darin aus, daß er seine die algebraischen Funktionen darstellenden Flächen als geschlossen betrachtet.

hauptung mehr enthält, also von der Wahrheit oder Unwahrheit derselben auch keine Rede sein kann. Unter den Funktionen des Körpers Ω finden sich außer unendlich vielen Veränderlichen auch sämtliche Konstanten, d. h. Zahlen. Hiernach gelangt man durch die oben gestellte Forderung zu folgendem Begriff.

1. Definition. Wenn alle Individuen $\alpha, \beta, \gamma, \ldots$ des Körpers Ω durch bestimmte Zahlwerte $\alpha_0, \beta_0, \gamma_0, \ldots$ so ersetzt werden, daß

$$\text{(I.)}\ \alpha_0 = \alpha, \text{ falls } \alpha \text{ konstant ist, und allgemein}$$

$$\text{(II.)}\ (\alpha+\beta)_0 = \alpha_0 + \beta_0, \qquad \text{(IV.)}\ (\alpha\beta)_0 = \alpha_0\beta_0,$$

$$\text{(III.)}\ (\alpha-\beta)_0 = \alpha_0 - \beta_0, \qquad \text{(V.)}\ \left(\frac{\alpha}{\beta}\right)_0 = \frac{\alpha_0}{\beta_0}$$

wird, so soll einem solchen Zusammentreffen bestimmter Werte ein Punkt $\mathfrak{P}$ zugeordnet werden [den man sich zur Versinnlichung irgendwie im Raume gelegen vorstellen mag *)], und wir sagen, in $\mathfrak{P}$ sei $\alpha = \alpha_0$, oder α habe in $\mathfrak{P}$ den Wert α_0. Zwei Punkte heißen stets und nur dann verschieden, wenn eine Funktion α in Ω existiert, die in beiden Punkten verschiedene Werte hat.

Aus dieser Definition des Punktes soll nun die Existenz desselben, sowie der Umfang des Begriffes deduziert werden. Zunächst ist aber hervorzuheben, daß nach dieser Definition der „Punkt“ ein zum Körper Ω gehöriger invarianter Begriff ist, der in keiner Weise abhängt von der Wahl der unabhängigen Veränderlichen, durch welche man die Funktionen des Körpers darstellt.

2. Satz. Ist ein Punkt $\mathfrak{P}$ gegeben, und z eine in $\mathfrak{P}$ endliche Variable in Ω (eine solche existiert für jeden Punkt; denn ist $z_0 = \infty$, so ist $\left(\frac{1}{z}\right)_0 = 0$, also endlich), so hat auch jede ganze Funktion ω von z in $\mathfrak{P}$ einen endlichen Wert ω_0 — denn zwischen ω und z besteht eine Relation von der Form

$$1 = a\frac{1}{\omega} + b\frac{1}{\omega^2} + \cdots + k\frac{1}{\omega^m},$$

*) Eine geometrische Versinnlichung des „Punktes“ ist übrigens keineswegs notwendig und trägt zu einer leichteren Auffassung nicht einmal viel bei. Es genügt, das Wort „Punkt“ als einen kurzen und bequemen Ausdruck für die beschriebene Wert-Koexistenz zu betrachten.

worin $a, b, \ldots k$ als ganze rationale Funktionen von z nach (II.), (III.), (IV.) in $\mathfrak{P}$ endliche Werte haben. Mithin kann $\left(\frac{1}{\omega}\right)_0$ nicht gleich 0, also ω_0 nicht gleich ∞ sein.

3. Satz. Ist z irgendeine in $\mathfrak{P}$ endliche Variable, so ist der Inbegriff $\mathfrak{p}$ aller derjenigen ganzen Funktionen π von z, welche in $\mathfrak{P}$ verschwinden, ein Primideal in z; wir sagen, der Punkt $\mathfrak{P}$ erzeuge dies Primideal $\mathfrak{p}$. Ist ω eine ganze Funktion von z, welche in $\mathfrak{P}$ den Wert ω_0 hat, so ist $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$.

Beweis. Ist $\pi_0' = 0, \pi_0'' = 0$, so ist auch $(\pi' + \pi'')_0 = \pi_0' + \pi_0'' = 0$, und wenn ω eine beliebige ganze Funktion von z, also ω_0 endlich ist, so folgt aus $\pi_0 = 0$ auch $(\omega\pi)_0 = \omega_0 \pi_0 = 0$; also ist $\mathfrak{p}$ ein Ideal in z (§ 7, I., II.). Das Ideal $\mathfrak{p}$ ist von 0 verschieden, da es die Funktion „1“ nicht enthält.

Hat ω in $\mathfrak{P}$ den Wert ω_0, so ist $(\omega - \omega_0)_0 = 0$, folglich $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$, also jede ganze Funktion von z einer Konstanten kongruent nach dem Modul $\mathfrak{p}$. Daher ist (§ 9, 7.) $\mathfrak{p}$ ein Primideal.

4. Satz. Dasselbe Primideal $\mathfrak{p}$ kann nicht durch zwei verschiedene Punkte erzeugt werden.

Denn zunächst ist der Wert einer jeden ganzen Funktion ω in einem das Ideal $\mathfrak{p}$ erzeugenden Punkt $\mathfrak{P}$ durch die Kongruenz $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$ vollkommen bestimmt. Ist aber η eine beliebige Funktion in Ω, so lassen sich nach § 12, 1. zwei ganze Funktionen α, β, die nicht beide durch $\mathfrak{p}$ teilbar sind, so bestimmen, daß

$$\eta = \frac{\alpha}{\beta}$$

wird. Da nun die endlichen Werte α_0, β_0 nicht beide verschwinden, so folgt aus (V.)

$$\eta_0 = \frac{\alpha_0}{\beta_0},$$

also ebenfalls durch $\mathfrak{p}$ vollkommen bestimmt.

Es ergibt sich hieraus noch, daß zwei Punkte, in denen eine Variable z endliche Werte hat, dann und nur dann voneinander verschieden sind, wenn eine ganze Funktion von z existiert, welche in beiden verschiedene Werte hat.

5. Satz. Ist z irgendeine Variable in Ω und $\mathfrak{p}$ ein Primideal in z, so gibt es einen (und nach 4. auch nur einen) Punkt $\mathfrak{P}$,

welcher dies Primideal erzeugt, und welcher der Nullpunkt des Ideals $\mathfrak{p}$ genannt werden soll.

Beweis. Es sei η eine beliebige Funktion in Ω, und ϱ eine solche, deren Oberideal durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist. Es lassen sich dann nach § 12, 6. stets und nur auf eine Weise eine ganze Zahl m, eine von Null verschiedene endliche Konstante c und eine Funktion η_1, deren Unterideal nicht durch $\mathfrak{p}$ teilbar ist, so bestimmen, daß

$$\eta = c\,\varrho^m + \eta_1\,\varrho^{m+1}.$$

Wir setzen

$$\eta_0 = 0, \quad c, \quad \infty,$$

je nachdem m positiv, Null oder negativ ist. Dieser Wertbestimmung der Funktionen des Körpers Ω entspricht ein Punkt $\mathfrak{P}$, da die Bedingungen (I.) bis (V.), wie man sofort übersieht, erfüllt sind*).

Jede Funktion, deren Oberideal durch $\mathfrak{p}$ teilbar ist, also insbesondere jede Funktion in $\mathfrak{p}$ erhält nach dieser Festsetzung in $\mathfrak{P}$ den Wert Null, d. h. der so bestimmte Punkt $\mathfrak{P}$ erzeugt das Primideal $\mathfrak{p}$.

Jede Funktion, deren Unterideal durch $\mathfrak{p}$ teilbar ist, und nur eine solche hat in $\mathfrak{P}$ den Wert ∞, und daraus geht hervor, daß eine ganze Funktion von z in keinem Punkte, in welchem z einen endlichen Wert hat, unendlich ist, und, da eine gebrochene Funktion von z im Unterideal gewiß ein Primideal enthält, also mindestens in einem Punkte, in welchem z endlich ist, unendlich sein muß, so ist auch umgekehrt jede Funktion, die in keinem Punkte, in welchem z einen endlichen Wert hat, unendlich ist, eine ganze Funktion von z.

6. Aus 3., 4., 5. ergibt sich nun das folgende Resultat. Um alle existierenden Punkte $\mathfrak{P}$ und jeden nur ein einziges Mal zu erhalten, ergreife man eine beliebige Variable z des Körpers Ω; man bilde alle Primideale $\mathfrak{p}$ in z und konstruiere für jedes derselben den Nullpunkt, so sind alle diejenigen Punkte $\mathfrak{P}$ gefunden, in denen z

---

*) Ist $\eta' = c'\varrho^{m'} + \eta_1'\varrho^{m'+1}$, so ist z. B.

$$\frac{\eta}{\eta'} = \varrho^{m-m'}\left(\frac{c}{c'} + \varrho\,\eta_1''\right),$$

worin

$$\eta_1'' = \frac{c'\eta_1 - c\eta_1'}{c'(c' + \varrho\,\eta_1')}$$

eine Funktion von derselben Beschaffenheit ist wie η_1 (noch einfacher ist der Beweis in den übrigen Fällen).

endlich bleibt; ist $\mathfrak{P}'$ ein von diesen verschiedener Punkt, so hat in ihm $z' = \frac{1}{z}$ den endlichen Wert Null; umgekehrt ist jeder Punkt $\mathfrak{P}'$, in dem z' den Wert Null hat, von den Punkten $\mathfrak{P}$ verschieden. Das durch einen solchen Punkt $\mathfrak{P}'$ erzeugte Primideal $\mathfrak{p}'$ in z' (welches aus allen in $\mathfrak{P}'$ verschwindenden ganzen Funktionen von z' besteht) geht in z' auf, und umgekehrt ist der Nullpunkt eines jeden in z' aufgehenden Primideals $\mathfrak{p}'$ in z' ein Punkt $\mathfrak{P}'$, in welchem $z' = 0$ also $z = \infty$ ist. Mit diesen in endlicher Anzahl vorhandenen, den verschiedenen $\mathfrak{p}'$ entsprechenden Ergänzungspunkten und den vorher aus den Primidealen $\mathfrak{p}$ in z abgeleiteten ist die Gesamtheit aller Punkte $\mathfrak{P}$ erschöpft, deren Inbegriff die Riemannsche Fläche T bildet.

§ 15.

Die Ordnungszahlen.

1. Definition. Ist $\mathfrak{P}$ ein bestimmter Punkt, so betrachten wir die sämtlichen in $\mathfrak{P}$ verschwindenden Funktionen π in Ω, und erteilen jeder derselben eine bestimmte Ordnungszahl nach folgendem Gesichtspunkt.

Eine solche Funktion ϱ hat die Ordnungszahl 1, oder heißt unendlich klein in der ersten Ordnung oder 0^1 in $\mathfrak{P}$, wenn alle Quotienten $\frac{\pi}{\varrho}$ in $\mathfrak{P}$ endlich bleiben. Ist ϱ' eine ebensolche Funktion wie ϱ, so ist $\frac{\varrho'}{\varrho}$ in $\mathfrak{P}$ weder 0 noch ∞, und umgekehrt, ist $\frac{\varrho'}{\varrho}$ in $\mathfrak{P}$ weder 0 noch ∞, so ist ϱ' gleichfalls unendlich klein von der ersten Ordnung. Gibt es ferner für irgendeine Funktion π einen ganzen positiven Exponenten r, so daß $\frac{\pi}{\varrho^r}$ in $\mathfrak{P}$ weder 0 noch ∞ wird, so gilt dasselbe von $\frac{\pi}{\varrho'^r}$, und π erhält die Ordnungszahl r oder heißt unendlich klein in der Ordnung r im Punkte $\mathfrak{P}$. Wir werden auch sagen, π ist 0^r in $\mathfrak{P}$ oder π ist 0 in $\mathfrak{P}^r$.

Um die Frage nach der Existenz solcher Funktionen ϱ und solcher Ordnungszahlen r zu entscheiden, ergreife man eine beliebige in $\mathfrak{P}$ endliche Variable z, bezeichne mit $\mathfrak{p}$ das durch $\mathfrak{P}$ erzeugte Primideal in z, und stelle jede Funktion π (mit Ausnahme der ordnungslosen Konstanten 0) nach § 12 als Quotienten von zwei

relativen Primidealen in z dar. Das Oberideal jeder dieser Funktionen ist dann durch $\mathfrak{p}$ teilbar, und es gibt darunter auch solche, deren Oberideal nicht durch $\mathfrak{p}^2$ teilbar ist; diese haben die Ordnungszahl 1; für die übrigen Funktionen π ist die Ordnungszahl der Exponent der höchsten im Oberideal aufgehenden Potenz von $\mathfrak{p}$, was sich aus den Sätzen des § 12 ohne weiteres ergibt.

2. Hat eine Funktion η den endlichen Wert η_0 in $\mathfrak{P}$, so sagen wir, η habe diesen Wert r-mal in $\mathfrak{P}$ oder in r mit $\mathfrak{P}$ zusammenfallenden Punkten oder in $\mathfrak{P}^r$, wenn die Funktion $\eta - \eta_0$ in $\mathfrak{P}$ unendlich klein in der Ordnung r ist. Ist aber $\eta_0 = \infty$, so sagen wir, η habe den Wert ∞ r-mal in $\mathfrak{P}$ oder in r mit $\mathfrak{P}$ zusammenfallenden Punkten, oder η sei ∞^r in $\mathfrak{P}$ oder ∞ in $\mathfrak{P}^r$, wenn $\frac{1}{\eta}$ in $\mathfrak{P}^r$ verschwindet.

3. Wird eine Funktion η in $\mathfrak{P}$ ∞^r, so legen wir derselben auch die Ordnungszahl $-r$ bei, wenn aber η in $\mathfrak{P}$ weder 0 noch ∞ wird, so habe sie die Ordnungszahl 0. Hiernach kommt in einem beliebigen Punkte $\mathfrak{P}$ jeder Funktion des Körpers Ω eine ganz bestimmte Ordnungszahl zu, mit Ausnahme der beiden Konstanten 0 und ∞.

4. Ist ϱ eine Funktion, welche in einem beliebigen Punkte $\mathfrak{P}$ die Ordnungszahl 1 besitzt, und η eine Funktion mit der (positiven, negativen oder verschwindenden) Ordnungszahl m, so läßt sich nach dem Schlußsatz des § 12 für jedes beliebige positive r eine Reihe von Konstanten $c_0, c_1, \ldots c_{r-1}$, deren erste nicht verschwindet, und eine in $\mathfrak{P}$ endliche Funktion σ so bestimmen, daß

$$\eta = c_0 \varrho^m + c_1 \varrho^{m-1} + \cdots + c_{r-1} \varrho^{m+r-1} + \sigma \varrho^{m+r}$$

wird.

5. Hieraus ergibt sich unmittelbar, daß die Ordnungszahl eines Produktes zweier oder mehrerer Funktionen gleich ist der Summe der Ordnungszahlen der einzelnen Faktoren.

Die Ordnungszahl eines Quotienten zweier Funktionen ist gleich der Differenz der Ordnungszahlen des Zählers und Nenners.

Ist $\eta_1, \eta_2, \ldots \eta_s$ eine Reihe von Funktionen und m die algebraisch kleinste unter ihren Ordnungszahlen, so ist

$$\begin{aligned}
\eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\
\eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\
&\cdots\cdots\cdots\cdots \\
\eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1},
\end{aligned}$$

worin die Konstanten $e_1, e_2, \dots e_s$ jedenfalls nicht alle verschwinden. Sind daher $c_1, c_2, \dots c_s$ Konstanten, so ist die Ordnungszahl von

$$\eta = c_1\eta_1 + c_2\eta_2 + \cdots + c_s\eta_s,$$

falls $c_1 e_1 + c_2 e_2 + \cdots + c_s e_s$ von Null verschieden ist, ebenfalls m, sonst größer als m.

6. Komplexe von Punkten, welche denselben Punkt auch mehrmals enthalten können, nennen wir Polygone und bezeichnen dieselben mit $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$

Es bedeute ferner $\mathfrak{A}\mathfrak{B}$ das aus den Punkten von $\mathfrak{A}$ und von $\mathfrak{B}$ zusammengesetzte Polygon in der Weise, daß, wenn ein Punkt $\mathfrak{P}$ r-mal in $\mathfrak{A}$, s-mal in $\mathfrak{B}$ auftritt, er $(r+s)$-mal in $\mathfrak{A}\mathfrak{B}$ vorkommt. Daraus ergibt sich die Bedeutung von $\mathfrak{P}^r$ und von $\mathfrak{A} = \mathfrak{P}^r \mathfrak{P}_1^{r_1} \mathfrak{P}_2^{r_2} \dots$, und die Gesetze der Teilbarkeit der Polygone in vollkommener Übereinstimmung mit denen der Teilbarkeit der ganzen Zahlen und der Ideale. Die Rolle der Primfaktoren übernehmen dabei die Punkte; um aber auch die Einheit zu erhalten, muß man das gar keinen Punkt enthaltende Polygon $\mathfrak{O}$ (das Nulleck) zulassen.

Die Anzahl der Punkte eines Polygons heißt seine Ordnung. Ein Polygon von der Ordnung n wird auch kurz ein n-Eck genannt.

Der größte gemeinschaftliche Teiler zweier Polygone $\mathfrak{A}, \mathfrak{B}$ ist dasjenige Polygon, welches jeden Punkt $\mathfrak{P}$ so oft enthält, als er in $\mathfrak{A}$ und $\mathfrak{B}$ mindestens vorkommt. Ist dies $\mathfrak{O}$, so heißen $\mathfrak{A}, \mathfrak{B}$ relativ prim.

Das kleinste gemeinschaftliche Vielfache von $\mathfrak{A}$ und $\mathfrak{B}$ ist dasjenige Polygon, welches jeden Punkt so oft enthält, als er in $\mathfrak{A}$ und $\mathfrak{B}$ höchstens vorkommt. Sind $\mathfrak{A}, \mathfrak{B}$ relativ prim, so ist $\mathfrak{A}\mathfrak{B}$ ihr kleinstes gemeinschaftliches Vielfache.

Ist $\mathfrak{A} = \mathfrak{P}^r \mathfrak{P}_1^{r_1} \mathfrak{P}_2^{r_2} \dots$ ein beliebiges Polygon, so gibt es stets Funktionen z in Ω, welche in keinem der Punkte $\mathfrak{A}$ unendlich sind. Denn wenn z in einigen Punkten von $\mathfrak{A}$ unendlich ist, so kann man eine Konstante c so wählen, daß $z - c$ in keinem der Punkte von $\mathfrak{A}$ den Wert 0 hat, und dann ist $\frac{1}{z-c}$ in allen Punkten des Polygons $\mathfrak{A}$ endlich. Legt man eine solche Variable z zugrunde, so ist der Inbegriff aller derjenigen ganzen Funktionen von z, welche in den Punkten des Polygons $\mathfrak{A}$ (jeden nach seiner Vielfachheit gezählt) verschwinden, ein Ideal $\mathfrak{a} = \mathfrak{p}^r \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \dots$, und man kann sagen, das Polygon $\mathfrak{A}$ erzeuge das Ideal $\mathfrak{a}$, oder $\mathfrak{A}$ sei das Nullpolygon des

Ideals $\mathfrak{a}$. Der Idealbegriff fällt hiernach vollständig zusammen mit dem Begriff eines Systems ganzer Funktionen, welche alle in denselben festen Punkten verschwinden. Das Ideal $\mathfrak{o}$ wird erzeugt durch das Nulleck $\mathfrak{O}$.

Das Produkt zweier oder mehrerer Ideale wird erzeugt durch das Produkt der Nullpolygone der Faktoren, größter gemeinschaftlicher Teiler und kleinstes gemeinschaftliches Vielfache zweier Ideale durch den größten gemeinschaftlichen Teiler und das kleinste gemeinschaftliche Vielfache der entsprechenden Nullpolygone.

7. Satz. Ist z irgendeine Variable in Ω und n der Grad des Körpers Ω in bezug auf z, so nimmt z jeden bestimmten Wert c in genau n Punkten an. — Denn wenn $\mathfrak{o}$ das System aller ganzen Funktionen von z und c eine endliche Konstante bedeutet, so ist

$$\mathfrak{o}(z-c) = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\ldots, \qquad e_1 + e_2 + \cdots = n \quad (\S\ 9,\ 7.),$$

wenn $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ voneinander verschiedene Primideale in z bedeuten. Bezeichnet man mit $\mathfrak{P}_1, \mathfrak{P}_2, \ldots$ die Nullpunkte von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$, so hat nach 2. z den Wert c in e_1 Punkten $\mathfrak{P}_1$ (oder in $\mathfrak{P}_1^{e_1}$), in e_2 Punkten $\mathfrak{P}_2$ (oder in $\mathfrak{P}_2^{e_2}$) usf., also in den n Punkten des Polygons $\mathfrak{P}_1^{e_1}\,\mathfrak{P}_2^{e_2}\ldots$ Umgekehrt: ist $\mathfrak{P}$ ein Punkt, in welchem z den Wert c hat, und $\mathfrak{p}$ das durch $\mathfrak{P}$ erzeugte Primideal in z, so ist $z \equiv c \pmod{\mathfrak{p}}$, und folglich ist $\mathfrak{p}$ eines der Ideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$, mithin $\mathfrak{P}$ einer der Punkte $\mathfrak{P}_1\,\mathfrak{P}_2\ldots$ Dasselbe Resultat gilt aber auch für $c = \infty$; denn weil n auch der Grad von Ω in bezug auf $\frac{1}{z}$ ist, so nimmt letztere Variable den Wert 0, folglich z den Wert ∞ in genau n Punkten an. Aus § 11 folgt, daß nur für eine endliche Anzahl von Werten der Konstanten c einer der Exponenten $e_1, e_2, \ldots$ größer als 1 sein kann.

Die Zahl n, d. h. die Anzahl der Punkte, in welchen die Funktion z je einen konstanten Wert hat, soll die **Ordnung** der Funktion z genannt werden. Die Konstanten und nur diese haben die Ordnung Null. Für alle anderen Funktionen in Ω ist die Ordnung eine positive ganze Zahl. Die Ordnung einer Variablen z ist zugleich der Grad des Körpers Ω in bezug auf z.

§ 16.

Konjugierte Punkte und konjugierte Werte.

1. Definition. Ist c ein bestimmter Zahlwert, so entspricht demselben, wie in § 15 gezeigt, ein Polygon $\mathfrak{A}$ von n (gleichen oder

verschiedenen) Punkten $\mathfrak{P}', \mathfrak{P}'', \ldots \mathfrak{P}^{(n)}$, in welchen die Variable n^{ter} Ordnung z eben diesen Wert hat; diese n Punkte sollen **konjugiert nach** z heißen; durch einen von ihnen (und durch die Variable z) sind die übrigen bestimmt. Läßt man c nach und nach alle Werte annehmen, so bewegt sich das Polygon $\mathfrak{A} = \mathfrak{P}' \mathfrak{P}'' \ldots \mathfrak{P}^{(n)}$, und zwar so, daß stets alle seine Punkte sich verändern. Man erhält hierbei also alle überhaupt existierenden Punkte und nur diejenigen (in endlicher Anzahl vorhandenen) mehrfach, in welchen $z - z_0$ oder $\frac{1}{z}$ in höherer als der ersten Ordnung verschwindet. Es ist daher das Produkt aller dieser Polygone

$$\Pi \mathfrak{A} = T \mathfrak{Z}_z,$$

wo T die einfache Gesamtheit aller Punkte, die **Riemannsche Fläche**, $\mathfrak{Z}_z$ ein bestimmtes endliches Polygon ist, welches das **Verzweigungs- oder Windungspolygon von** T **in** z heißt. Jeder in $\mathfrak{Z}_z$ enthaltene Punkt $\mathfrak{O}$ heißt ein **Verzweigungs- oder Windungspunkt von** T **in** z, und zwar von der Ordnung s, wenn er genau s-mal in $\mathfrak{Z}_z$ vorkommt. Es ist $s = e - 1$, wenn $z - z_0$ oder $\frac{1}{z}$ in $\mathfrak{O}$ unendlich klein von der e^{ten} Ordnung ist. Die Ordnung des Polygons $\mathfrak{Z}_z$ heißt die **Verzweigungs- oder Windungszahl** $\mathfrak{w}_z$ der Fläche T nach z. Diejenigen Punkte des Verzweigungspolygons, in welchen z einen endlichen Wert hat, erzeugen zusammen das **Verzweigungsideal in** z (§ 11).

Will man von dieser Definition der „absoluten" Riemannschen Fläche, welche ein zu dem Körper Ω gehöriger invarianter Begriff ist, zu der bekannten Riemannschen Vorstellung übergehen, so hat man sich die Fläche in einer z-Ebene ausgebreitet zu denken, welche sie dann überall mit Ausnahme der Verzweigungspunkte n-fach bedeckt.

2. Satz. Ist

$$z' = \frac{c + dz}{a + bz},$$

worin a, b, c, d Konstanten bedeuten, deren Determinante $ad - bc$ von Null verschieden ist, so ist

$$\mathfrak{Z}_z = \mathfrak{Z}_{z'}; \quad \mathfrak{w}_z = \mathfrak{w}_{z'}.$$

Denn wenn in einem Punkte $\mathfrak{P}$ $z - z_0$ oder $\frac{1}{z}$ unendlich klein in der e^{ten} Ordnung ist, so ist in demselben Punkte auch

$$z' - z_0' = \frac{(ad - bc)(z - z_0)}{(a + bz)(a + bz_0)},$$

oder falls z_0 unendlich ist:

$$z' - z_0' = \frac{-(ad - bc)}{b(a + bz)},$$

oder falls $z_0' = \infty$, also $a + bz_0 = 0$ ist:

$$\frac{1}{z'} = \frac{a + bz}{c + dz}$$

unendlich klein in der e^{ten} Ordnung.

Ist insbesondere $z' = \frac{1}{z}$, so ist die Verzweigungszahl $\mathfrak{w}_z = \mathfrak{w}_{z'}$ gleich dem Grade der Diskriminante $\Delta_z(\Omega)$ vermehrt um die Anzahl der verschwindenden Wurzeln von $\Delta_{z'}(\Omega) = 0$ (§ 11).

3. **Definition.** Die Werte $\eta', \eta'', \ldots \eta^{(n)}$, welche eine beliebige Funktion η in Ω in n nach z konjugierten Punkten $\mathfrak{P}', \mathfrak{P}'', \ldots \mathfrak{P}^{(n)}$ annimmt, heißen **konjugierte Werte von η nach z.**

4. **Satz.** Ist $N_z(\eta)$ die Norm einer beliebigen Funktion in bezug auf z, so ist der Wert, welchen diese rationale Funktion von z für $z = z_0$ besitzt, gleich dem Produkt $\eta' \eta'' \ldots \eta^{(n)}$ der zu $z = z_0$ gehörigen konjugierten Werte von η, wobei von dem Falle, daß dies Produkt unbestimmt wird, also einer dieser konjugierten Werte 0, ein anderer ∞ ist, abzusehen ist. Beim Beweis dieses Satzes können wir annehmen, es sei z_0 endlich; denn ist $z_0 = \infty$, so legen wir statt z die Variable $z' = \frac{1}{z}$ zugrunde, wobei die Norm ungeändert bleibt. Ferner können wir annehmen, die Werte $\eta', \eta'', \ldots \eta^{(n)}$ seien alle endlich; denn ist einer von ihnen unendlich, so ist n. V. keiner derselben gleich 0, und wir betrachten statt η die Funktion $\frac{1}{\eta}$.

Es sei nun unter diesen Voraussetzungen

$$o(z - z_0) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \ldots$$

und $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \ldots$ die Nullpunkte der voneinander verschiedenen Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ Wir konstruieren ein System ganzer Funktionen λ, μ von z nach folgender Regel:

Es sei

$$\begin{array}{llllll}
\lambda_1 & \text{teilbar durch} & \mathfrak{p}_1, & \text{nicht durch} & \mathfrak{p}_1^2; \\
\lambda_2 & \text{„} & \text{„} & \mathfrak{p}_2, & \text{„} & \text{„} & \mathfrak{p}_2^2; \\
\lambda_3 & \text{„} & \text{„} & \mathfrak{p}_3, & \text{„} & \text{„} & \mathfrak{p}_3^2; \\
\multicolumn{6}{c}{\dotfill}
\end{array}$$

$$\begin{array}{llllll}
\mu_1 & \text{teilbar durch} & \mathfrak{p}_2^{e_2}, \mathfrak{p}_3^{e_3}, \ldots, & \text{nicht durch} & \mathfrak{p}_1, \mathfrak{p}_2^{e_2+1}, \mathfrak{p}_3^{e_3+1}, \ldots; \\
\mu_2 & \text{„} & \text{„} & \mathfrak{p}_1^{e_1}, \mathfrak{p}_3^{e_3}, \ldots; & \text{„} & \text{„} & \mathfrak{p}_2, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_3^{e_3+1}, \ldots; \\
\mu_3 & \text{„} & \text{„} & \mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2}, \ldots, & \text{„} & \text{„} & \mathfrak{p}_3, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_2^{e_2+1}, \ldots\text{*}). \\
\multicolumn{6}{c}{\dotfill}
\end{array}$$

Die n Funktionen

$$\begin{array}{llll}
\mu_1, & \mu_1\lambda_1, & \mu_1\lambda_1^2, & \ldots \quad \mu_1\lambda_1^{e_1-1}, \\
\mu_2, & \mu_2\lambda_2, & \mu_2\lambda_2^2, & \ldots \quad \mu_2\lambda_2^{e_2-1}, \\
\mu_3, & \mu_3\lambda_3, & \mu_3\lambda_3^2, & \ldots \quad \mu_3\lambda_3^{e_3-1}, \\
\multicolumn{4}{c}{\dotfill}
\end{array}$$

die wir mit $\eta_1, \eta_2, \ldots \eta_n$ bezeichnen, bilden dann eine Basis von Ω; diese Behauptung ist in der nun zu beweisenden allgemeineren enthalten.

Wenn

$$(z - z_0)\,\zeta = x_1\eta_1 + x_2\eta_2 + \cdots + x_n\eta_n$$

mit ganzen rationalen Koeffizienten $x_1, x_2, \ldots x_n$ ist, und ζ in den Punkten $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \ldots$ endliche Werte $\zeta', \zeta'', \zeta''', \ldots$ hat, so müssen die sämtlichen Koeffizienten $x_1, x_2, \ldots x_n$ durch $z - z_0$ teilbar sein In der Tat ist z. B. im Punkte $\mathfrak{P}_1$ die linke Seite unendlich klein mindestens in der Ordnung e_1. Es muß also nach § 15, 5. auch

$$x_1\eta_1 + x_2\eta_2 + \cdots + x_{e_1}\eta_{e_1} = \mu_1(x_1 + x_2\lambda_1 + \cdots + x_{e_1}\lambda_1^{e_1-1})$$

in dieser Ordnung unendlich klein sein. Dies ist aber nur möglich, wenn $x_1, x_2, \ldots x_{e_1}$ in $\mathfrak{P}_1$ verschwinden, also durch $z - z_0$ teilbar sind, w. z. b. w.

Hiernach können wir setzen:

$$\begin{aligned}
\eta\,\mu_1\lambda_1^r = {} & \mu_1(x_1^{(0)} + x_1^{(1)}\lambda_1 + \cdots + x_1^{(e_1-1)}\lambda_1^{e_1-1}) \\
& + \mu_2(x_2^{(0)} + x_2^{(1)}\lambda_2 + \cdots + x_2^{(e_2-1)}\lambda_2^{e_2-1}) \\
& + \mu_3(x_3^{(0)} + x_3^{(1)}\lambda_3 + \cdots + x_3^{(e_3-1)}\lambda_3^{e_3-1}) + \cdots,
\end{aligned}$$

worin die $x_1^{(0)}, x_1^{(1)}, \ldots x_2^{(0)}, \ldots$ rationale Funktionen von z sind, die alle für $z - z_0$ endlich bleiben. In den Punkten $\mathfrak{P}_2, \mathfrak{P}_3, \ldots$ ist die linke

*) Die Möglichkeit, solche Funktionen zu bestimmen, ergibt sich aus § 9, 3., Anmerkung, oder auch nach § 11, 2., wonach man z. B. setzen kann

$$\lambda = \varrho - b, \quad \mu\lambda^e = \psi(\varrho).$$

Seite unendlich klein mindestens in der Ordnung $e_2, e_3, \ldots$ Dasselbe gilt für $\mathfrak{P}_2$ von $\mu_1, \mu_3, \ldots$, aber nicht von μ_2, für $\mathfrak{P}_3$ von $\mu_1, \mu_2, \ldots$ aber nicht von $\mu_3, \ldots$; folglich ist für $z = z_0$

$$x_2^{(0)} = 0, \quad x_2^{(1)} = 0, \quad \ldots \quad x_2^{(e_2-1)} = 0,$$
$$x_3^{(0)} = 0, \quad x_3^{(1)} = 0, \quad \ldots \quad x_3^{(e_3-1)} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

In $\mathfrak{P}_1$ ist die linke Seite unendlich klein mindestens in der Ordnung r; daher wird, wenn $r < e_1$ ist, für $z = z_0$

$$x_1^{(0)} = 0, \quad x_1^{(1)} = 0, \quad \ldots \quad x_1^{(r-1)} = 0, \quad x_1^{(r)} = \eta'.$$

Dieselbe Betrachtung läßt sich auf die Funktionen $\eta\,\mu_2\,\lambda_2^r$, $\eta\,\mu_3\,\lambda_3^r, \cdots$ anwenden. Setzt man also

$$\eta\,\eta_1 = x_{1,1}\,\eta_1 + x_{1,2}\,\eta_2 + \cdots + x_{1,n}\,\eta_n,$$
$$\eta\,\eta_2 = x_{2,1}\,\eta_1 + x_{2,2}\,\eta_2 + \cdots + x_{2,n}\,\eta_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\eta\,\eta_n = x_{n,1}\,\eta_1 + x_{n,2}\,\eta_2 + \cdots + x_{n,n}\,\eta_n,$$

so werden in der Determinante

$$N(\eta) = \Sigma \pm x_{1,1}\,x_{2,2} \ldots x_{n,n}$$

sämtliche links von der Diagonalreihe stehenden Glieder für $z = z_0$ verschwinden, während von den Diagonalgliedern e_1 gleich η', e_2 gleich η'', e_3 gleich η''', ... werden. Es ist also für $z = z_0$

$$N(\eta) = \eta'^{e_1}\,\eta''^{e_2}\,\eta'''^{e_3} \ldots$$

w. z. b. w.

5. Da nach der Definition der Spur (§ 2)

$$S(\eta) = x_{1,1} + x_{2,2} + \cdots + x_{n,n}$$

ist, so führen dieselben Betrachtungen zu dem Satze:

Es ist für $z = z_0$

$$S(\eta) = e_1\,\eta' + e_2\,\eta'' + e_3\,\eta''' + \cdots,$$

welcher jedoch nur unter der Voraussetzung gilt, daß die Werte $\eta', \eta'', \eta''', \ldots$ endlich sind.

Der Satz 4. ergibt für ein beliebiges konstantes (oder rational von z abhängiges) t für $z = z_0$.

$$N(t - \eta) = (t - \eta')^{e_1}\,(t - \eta'')^{e_2}\,(t - \eta''')^{e_3} \ldots,$$

und daraus durch Vergleichung der Koeffizienten gleicher Potenzen von t für jeden dieser Koeffizienten einen Ausdruck durch die konjugierten Werte (symmetrische Funktionen).

6. Ist $\eta_1, \eta_2, \ldots \eta_n$ eine Basis von $\mathfrak{Q}$, so ergibt sich durch Anwendung von 5. sofort der Wert der Diskriminante dieses Systems für $z = z_0$

$$\Delta_z(\eta_1, \eta_2, \ldots \eta_n) = (\Sigma \pm \eta_1' \eta_2'' \ldots \eta_n^{(n)})^2,$$

wenn $\eta_i', \eta_i'', \ldots \eta_i^{(n)}$ die sämtlichen gleichen oder verschiedenen, aber als endlich vorausgesetzten, zu $z = z_0$ gehörigen konjugierten Werte von η_i bedeuten.

§ 17.

Darstellung der Funktionen des Körpers $\mathfrak{Q}$ durch Polygonquotienten.

Eine Funktion η des Körpers $\mathfrak{Q}$ hat nur in einer endlichen Anzahl von Punkten eine von Null verschiedene Ordnungszahl; die Summe sämtlicher Ordnungszahlen ist gleich 0, also die Summe der positiven gleich der Summe der negativen Ordnungszahlen, und zwar gleich der Ordnung der Funktion η (§ 15). Sind die Ordnungszahlen einer Funktion η für jeden Punkt $\mathfrak{P}$ bekannt, so ist damit die Funktion η bis auf einen konstanten Faktor bestimmt; denn hat η' überall dieselbe Ordnungszahl wie η, so hat $\frac{\eta}{\eta'}$ (nach § 15, 5.) überall die Ordnungszahl Null und ist also (nach § 15, 7.) eine Konstante.

Bilden wir also ein Polygon $\mathfrak{A}$, in welches wir jeden Punkt, in dem η eine positive Ordnungszahl hat, so oft aufnehmen, als diese Ordnungszahl angibt, und ein zweites Polygon $\mathfrak{B}$, in welches wir in entsprechender Weise die Punkte aufnehmen, in welchen η eine negative Ordnungszahl hat, so sind die Polygone $\mathfrak{A}$, $\mathfrak{B}$ von gleicher Ordnung, und zwar von der Ordnung der Funktion η. Durch diese Polygone $\mathfrak{A}$, $\mathfrak{B}$ ist also die Funktion η bis auf einen konstanten Faktor bestimmt. Wir setzen in symbolischer Bezeichnung

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

und nennen $\mathfrak{A}$ das Obereck, $\mathfrak{B}$ das Untereck der Funktion η*).

Nach dieser Festsetzung sind die beiden Polygone $\mathfrak{A}$, $\mathfrak{B}$ relativ prim; es ist aber zweckmäßig, die Bezeichnung dahin auszudehnen,

*) Alle Funktionen der einfachen Schar (η) haben hiernach dieselbe Bezeichnung $\frac{\mathfrak{A}}{\mathfrak{B}}$, und es würde daher korrekter sein, $(\eta) = \frac{\mathfrak{A}}{\mathfrak{B}}$ zu setzen; indessen führt diese Bezeichnung zu unnötigen Weitläufigkeiten.

daß man auch gemeinschaftliche Faktoren in $\mathfrak{A}$, $\mathfrak{B}$ zuläßt, was durch die Bestimmung geschieht, daß

$$\frac{\mathfrak{M}\mathfrak{A}}{\mathfrak{M}\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

sein soll, wenn $\mathfrak{M}$ ein beliebiges Polygon bedeutet. Setzen wir nach dieser verallgemeinerten Bezeichnung

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

so kann ein Punkt $\mathfrak{P}$, in welchem η die Ordnungszahl m besitzt, m_1-mal in $\mathfrak{A}$, m_2-mal in $\mathfrak{B}$ aufgenommen werden, wenn $m_1 - m_2 = m$ ist. Es ist auch jetzt noch die Ordnung von $\mathfrak{A}$ gleich der von $\mathfrak{B}$, aber nicht mehr gleich der Ordnung der Funktion η.

Aus dieser Definition ergibt sich (nach § 15, 5.) unmittelbar der Satz: Ist

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}}, \qquad \eta' = \frac{\mathfrak{A}'}{\mathfrak{B}'},$$

so ist

$$\eta\,\eta' = \frac{\mathfrak{A}\,\mathfrak{A}'}{\mathfrak{B}\,\mathfrak{B}'}, \quad \frac{\eta}{\eta'} = \frac{\mathfrak{A}\,\mathfrak{B}'}{\mathfrak{B}\,\mathfrak{A}'}.$$

Nach § 14, 5. ist eine Funktion η' dann und nur dann eine ganze Funktion von η, wenn jeder im Untereck von η' aufgehende Punkt auch in dem von η enthalten ist.

§ 18.

Äquivalente Polygone und Polygonklassen.

1. **Definition.** Zwei Polygone $\mathfrak{A}$, $\mathfrak{A}'$ von gleichviel Punkten heißen **äquivalent**, wenn eine Funktion η in Ω existiert, welche (nach § 17) die Bezeichnung hat:

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}.$$

2. **Satz.** Ist $\mathfrak{A}$ äquivalent mit $\mathfrak{A}'$ und mit $\mathfrak{A}''$, so ist auch $\mathfrak{A}'$ mit $\mathfrak{A}''$ äquivalent; denn aus

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{A}}; \quad \eta'' = \frac{\mathfrak{A}''}{\mathfrak{A}}$$

folgt:

$$\frac{\eta'}{\eta''} = \frac{\mathfrak{A}'}{\mathfrak{A}''}.$$

3. Definition und Satz. Alle mit einem gegebenen Polygon $\mathfrak{A}$ äquivalenten Polygone $\mathfrak{A}'$, $\mathfrak{A}''$, ... bilden eine Polygonklasse A. Nach 2. kommt dann jedes beliebige Polygon in einer und nur in einer Klasse vor; denn sind $\mathfrak{A}$, $\mathfrak{B}$ zwei äquivalente Polygone, welche zu den Klassen A, B führen, so ist nach 2. jedes Polygon der Klasse B zugleich in A enthalten und umgekehrt, und daher sind beide Klassen identisch.

Alle Polygone einer Klasse haben dieselbe Ordnung, welche die Ordnung der Klasse genannt werden soll.

4. Es können aber Polygone existieren, welche mit keinem anderen äquivalent sind, und deren jedes daher für sich eine Klasse bildet. Solche Polygone mögen isolierte genannt sein.

5. Ist $\mathfrak{M}$ ein beliebiges Polygon, und $\mathfrak{A}$ äquivalent mit $\mathfrak{A}'$, so ist auch $\mathfrak{M}\mathfrak{A}$ äquivalent mit $\mathfrak{M}\mathfrak{A}'$; aber auch umgekehrt folgt aus der Äquivalenz von $\mathfrak{M}\mathfrak{A}$ mit $\mathfrak{M}\mathfrak{A}'$ die Äquivalenz von $\mathfrak{A}$ mit $\mathfrak{A}'$.

6. Ist $\mathfrak{A}$ mit $\mathfrak{A}'$, $\mathfrak{B}$ mit $\mathfrak{B}'$ äquivalent, so ist auch $\mathfrak{A}\mathfrak{B}$ mit $\mathfrak{A}'\mathfrak{B}'$ äquivalent. Die Klasse C, welcher das Produkt $\mathfrak{A}\mathfrak{B}$ angehört, umfaßt daher die sämtlichen Produkte je zweier Polygone der Klassen A, B von $\mathfrak{A}$ und $\mathfrak{B}$ (aber außerdem unter Umständen noch unendlich viele andere Polygone) und soll als das Produkt der beiden Klassen A, B bezeichnet sein:

$$C = AB = BA.$$

Die Definition des Produkts von mehreren Klassen und die Gültigkeit des Fundamentalsatzes der Multiplikation ergibt sich hieraus von selbst.

7. Sind A, B, D drei Klassen, welche der Bedingung

$$DA = DB$$

genügen, so folgt $A = B$; denn sind $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{D}$ drei Polygone der Klassen A, B, D, so folgt aus der Voraussetzung, daß $\mathfrak{D}\mathfrak{B}$ mit $\mathfrak{D}\mathfrak{A}$, und folglich $\mathfrak{B}$ mit $\mathfrak{A}$ äquivalent ist.

8. Geht ein Polygon $\mathfrak{A}$ der Klasse A in einem Polygon $\mathfrak{C}$ der Klasse C auf, so gilt dasselbe von jedem Polygon $\mathfrak{A}'$ der Klasse A; denn aus $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ folgt nach 5., daß $\mathfrak{C}' = \mathfrak{A}'\mathfrak{B}$ in C enthalten ist, und wir können also, obschon nicht umgekehrt jedes Polygon der Klasse C durch ein Polygon der Klasse A teilbar zu sein braucht, sagen, die Klasse C sei durch die Klasse A teilbar. Ist $\mathfrak{B}'$ irgendein Polygon der Klasse B von $\mathfrak{B}$, so ist auch $\mathfrak{C}'' = \mathfrak{A}'\mathfrak{B}'$ in C enthalten und folglich

$$C = AB.$$

Ist also C durch A teilbar, so gibt es eine und (nach 7.) nur eine Klasse B, welche der Bedingung

$$C = AB$$

genügt.

§ 19.

Die Polygonscharen.

1. Sind $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ bestimmte, und zwar äquivalente Polygone, und $\mathfrak{A}$ ein beliebiges Polygon derselben Klasse A, so existieren s Funktionen in Ω

$$\eta_1 = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \eta_2 = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad \cdots \quad \eta_s = \frac{\mathfrak{A}_s}{\mathfrak{A}}.$$

Setzt man, wie in § 15, 5. für einen beliebigen Punkt $\mathfrak{P}$

$$\begin{aligned} \eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\ \eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\ &\cdots\cdots\cdots\cdots \\ \eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1}, \end{aligned}$$

worin ϱ in $\mathfrak{P}$ 0^1 ist, $e_1, e_2, \ldots e_s$ Konstanten, die nicht alle verschwinden, und $\sigma_1, \sigma_2, \ldots \sigma_s$ in $\mathfrak{P}$ endliche Funktionen bedeuten, so folgt, daß jede Funktion η der Schar $(\eta_1, \eta_2, \ldots \eta_s)$, d. h. jede Funktion von der Form

$$\eta = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s$$

in $\mathfrak{P}$ eine Ordnungszahl hat, die nicht kleiner als m ist, und daraus nach § 17, daß die Funktion η in die Form

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

gesetzt werden kann, wo $\mathfrak{A}'$ gleichfalls in der Klasse A enthalten ist.

Wählt man für $\mathfrak{A}$ ein beliebiges anderes Polygon $\mathfrak{B}$ der Klasse A, und setzt

$$\zeta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

$$\eta_1 \zeta = \eta_1' = \frac{\mathfrak{A}_1}{\mathfrak{B}}, \quad \eta_2 \zeta = \eta_2' = \frac{\mathfrak{A}_2}{\mathfrak{B}}, \quad \cdots \quad \eta_s \zeta = \eta_s' = \frac{\mathfrak{A}_s}{\mathfrak{B}},$$

so wird auch

$$\eta \zeta = \eta' = c_1 \eta_1' + c_2 \eta_2' + \cdots + c_s \eta_s',$$

und folglich

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{B}}.$$

Jedes durch den Nenner $\mathfrak{A}$ und ein Konstantensystem $c_1, c_2, \ldots c_s$ erzeugte Polygon wird daher auch durch jeden anderen derselben Klasse angehörigen Nenner $\mathfrak{B}$ erzeugt, und der Inbegriff der sämtlichen Polygone $\mathfrak{A}'$, die den verschiedenen Werten der Konstanten $c_1, c_2, \ldots c_s$ entsprechen, ist nur abhängig von den Polygonen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$. Dieser Inbegriff soll daher eine **Polygonschar** mit der Basis $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ genannt und mit

$$(\mathfrak{A}_1, \quad \mathfrak{A}_2, \quad \ldots \quad \mathfrak{A}_s)$$

bezeichnet werden.

2. Haben die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ einen größten gemeinschaftlichen Teiler $\mathfrak{M}$, so ist derselbe nach 1. auch Teiler eines jeden Polygons $\mathfrak{A}'$ der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$, und kann der **Teiler der Schar** genannt werden; aber es läßt sich in dieser Schar ein Polygon $\mathfrak{A}' = \mathfrak{M}\mathfrak{B}$ derart bestimmen, daß $\mathfrak{B}$ relativ prim zu einem beliebig gegebenen Polygon wird. Ist nämlich unter Beibehaltung der Bezeichnung von 1. ein Punkt $\mathfrak{P}$ genau μ-mal in $\mathfrak{M}$ und ν-mal in $\mathfrak{A}$ enthalten, so ist, wenn

$$\eta = e\varrho^m + \sigma\varrho^{m+1}$$

gesetzt wird, m niemals kleiner als $\mu - \nu$, und es ist $m = \mu - \nu$, wenn man die Konstanten $c_1, c_2, \ldots c_s$ so wählt, daß

$$e = c_1 e_1 + c_2 e_2 + \cdots + c_s e_s$$

von Null verschieden ist. Der Punkt $\mathfrak{P}$ ist daher mindestens μ-mal in $\mathfrak{A}'$ enthalten, und unter der letzteren Voraussetzung auch nicht öfter als μ-mal. Da man nun die Konstanten $c_1, c_2, \ldots c_s$ immer so wählen kann, daß eine beliebige Anzahl von Ausdrücken der Form

$$\Sigma c_\iota e_\iota, \quad \Sigma c_\iota e'_\iota, \quad \ldots,$$

in deren keinem die sämtlichen Konstanten $e_\iota, e'_\iota, \ldots$ verschwinden, von Null verschiedene Werte haben, so folgt die Richtigkeit der aufgestellten Behauptung.

3. Sind die Funktionen $\eta_1, \eta_2, \ldots \eta_s$ in 1. linear abhängig oder unabhängig, so gilt das gleiche von den Funktionen $\eta'_1, \eta'_2, \ldots \eta'_s$. Wir werden dementsprechend auch die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ **linear abhängig oder unabhängig** und ihr System **linear reduktibel oder irreduktibel nennen.**

Da nach § 5, 4. jede Funktionenschar eine irreduktible Basis besitzt, so folgt, daß auch jede Polygonschar eine **irreduktible Basis** hat. Ist s die Anzahl der Polygone einer solchen Basis, so

heißt die Schar eine s-fache, oder s die Dimension der Schar. Irgend s Polygone einer solchen Schar bilden eine irreduktible Basis derselben oder nicht, je nachdem sie linear unabhängig oder abhängig sind (vgl. § 5, 4.).

4. Sind die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ linear abhängig oder unabhängig, so sind, wenn $\mathfrak{M}$ ein beliebiges Polygon bedeutet, auch $\mathfrak{M}\mathfrak{A}_1, \mathfrak{M}\mathfrak{A}_2, \ldots \mathfrak{M}\mathfrak{A}_s$ linear abhängig oder unabhängig und umgekehrt.

§ 20.

Erniedrigung der Dimension der Schar durch Teilbarkeitsbedingungen.

1. Es sei

$$S = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$$

eine s-fache Schar vom Teiler $\mathfrak{M}$. Es wird nach der Mannigfaltigkeit derjenigen Polygone $\mathfrak{A}'$ der Schar S gefragt, welche einen beliebig gegebenen Punkt wenigstens einmal öfter enthalten als der Teiler $\mathfrak{M}$ der Schar.

Ist der Punkt $\mathfrak{P}$ μ-mal in $\mathfrak{M}$ und ν-mal in einem beliebigen mit $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ äquivalenten Polygon $\mathfrak{A}$ enthalten, so ist, wenn wir wie in § 19

$$\begin{aligned}
\frac{\mathfrak{A}_1}{\mathfrak{A}} &= \eta_1 = e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\
\frac{\mathfrak{A}_2}{\mathfrak{A}} &= \eta_2 = e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\
&\cdots\cdots\cdots\cdots\cdots \\
\frac{\mathfrak{A}_s}{\mathfrak{A}} &= \eta_s = e_s \varrho^m + \sigma_s \varrho^{m+1}
\end{aligned}$$

setzen, $m = \mu - \nu$, und von den Konstanten $e_1, e_2, \ldots e_s$ ist wenigstens eine, etwa e_s, von Null verschieden. Die gesuchten Polygone $\mathfrak{A}'$ sind dann durch die Gleichung charakterisiert

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = \eta' = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s,$$

worin die Konstanten $c_1, c_2, \ldots c_s$ an die Bedingung gebunden sind

$$c_1 e_1 + c_2 e_2 + \cdots + c_s e_s = 0.$$

Hiernach können wir setzen

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = e_s \eta' = c_1 (e_s \eta_1 - e_1 \eta_s) + \cdots + c_{s-1} (e_s \eta_{s-1} - e_{s-1} \eta_s).$$

Daraus aber ergibt sich, wenn wir

$$\begin{aligned}
\eta_1' &= e_s\eta_1 - e_1\eta_s,\\
\eta_2' &= e_s\eta_2 - e_2\eta_s,\\
&\cdots\cdots\cdots\cdots\\
\eta_{s-1}' &= e_s\eta_{s-1} - e_{s-1}\eta_s
\end{aligned}$$

setzen, daß die Funktionen η' eine $(s-1)$-fache Schar $(\eta_1', \eta_2', \ldots \eta_{s-1}')$ bilden; denn die Funktionen $\eta_1', \eta_2', \ldots \eta_{s-1}'$ sind linear unabhängig, wenn es, wie vorausgesetzt, die Funktionen $\eta_1, \eta_2, \ldots \eta_s$ sind. Es bilden also auch die Polygone $\mathfrak{A}'$ eine $(s-1)$-fache Schar

$$S' = (\mathfrak{A}_1', \mathfrak{A}_2', \ldots \mathfrak{A}_{s-1}'),$$

wenn

$$\frac{\mathfrak{A}_i'}{\mathfrak{A}} = e_s\eta_i - e_i\eta_s$$

gesetzt wird. Der Teiler dieser Schar ist durch $\mathfrak{M}\mathfrak{P}$ teilbar, wenn auch nicht notwendig damit identisch.

2. Hieraus ergibt sich sofort, daß die Polygone einer Schar S, welche durch ein beliebiges r-Eck $\mathfrak{R}$ teilbar sind, eine mindestens $(r-s)$-fache Schar bilden. Denn nehmen wir an, es sei dies bereits für ein r-Eck $\mathfrak{R}$ bewiesen, so folgt die Richtigkeit der Behauptung für ein $(r+1)$-Eck $\mathfrak{P}\mathfrak{R}$ unmittelbar aus 1., indem durch das Hinzutreten des Punktes $\mathfrak{P}$, wenn $\mathfrak{P}$ im Teiler der durch $\mathfrak{R}$ bereits reduzierten Schar enthalten ist, die Dimension nicht weiter geändert, sonst um 1 erniedrigt wird.

Hieraus folgt als Spezialfall, daß es in einer s-fachen Schar immer wenigstens ein Polygon gibt, welches durch ein gegebenes $(s-1)$-Eck teilbar ist.

3. Man kann, wenn $r \leqq s$ ist, das r-Eck $\mathfrak{R}$ so wählen, daß die durch $\mathfrak{R}$ teilbaren Polygone der Schar S eine genau $(s-r)$-fache Schar bilden. Zu diesem Ende wähle man einen Punkt $\mathfrak{P}$, welcher im Teiler von S nicht enthalten ist; die durch $\mathfrak{P}$ teilbaren Polygone in S bilden nach 1. eine $(s-1)$-fache Schar S'; man wähle einen zweiten Punkt $\mathfrak{P}'$, der nicht im Teiler von S' enthalten ist; die Polygone in S', die durch $\mathfrak{P}'$, d. h. die Polygone in S, die durch $\mathfrak{P}\mathfrak{P}'$ teilbar sind, bilden eine $(s-2)$-fache Schar, usf.; zugleich erhellt aus dieser Bildungsweise, daß man $\mathfrak{R}$ zu einem beliebig gegebenen Polygon relativ prim annehmen kann. Ist $r = s$, so wird hiernach in S kein durch $\mathfrak{R}$ teilbares Polygon existieren.

§ 21.

Die Dimensionen der Polygonklassen.

1. Die Polygone einer Klasse bilden eine Schar von endlicher Dimension, welche die Dimension der Klasse heißen soll.

Beweis. Wählt man in einer Klasse A, deren Ordnung m sei, irgend s Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ aus, so gehören alle Polygone der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$ zugleich in die Klasse A. Die Anzahl der linear unabhängigen Polygone, die in A enthalten sind, kann daher gewiß nicht größer sein als $m+1$, weil man sonst (nach § 20, 2.) in der Klasse ein durch ein beliebiges $(m+1)$-Eck teilbares Polygon finden könnte, was widersinnig ist. Wenn daher s die Maximalzahl der linear unabhängigen Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ der Klasse A ist, so muß jedes Polygon dieser Klasse in der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$ enthalten sein, und s ist die Dimension der Klasse. Das System der Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ soll eine Basis der Klasse genannt werden.

Die isolierten Polygone bilden Klassen von der Dimension 1.

2. Gibt es in einer Klasse C s und nicht mehr linear unabhängige, durch ein gegebenes Polygon $\mathfrak{A}$ der Klasse A teilbare Polygone

$$\mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1, \quad \mathfrak{C}_2 = \mathfrak{A}\mathfrak{B}_2, \quad \ldots \quad \mathfrak{C}_s = \mathfrak{A}\mathfrak{B}_s,$$

so ist C durch A teilbar, und es existieren in C auch ebenso viele linear unabhängige Polygone

$$\mathfrak{C}'_1 = \mathfrak{A}'\mathfrak{B}_1, \quad \mathfrak{C}'_2 = \mathfrak{A}'\mathfrak{B}_2, \quad \ldots \quad \mathfrak{C}'_s = \mathfrak{A}'\mathfrak{B}_s,$$

welche durch ein beliebiges mit $\mathfrak{A}$ äquivalentes Polygon $\mathfrak{A}'$ teilbar sind (§ 18, 8.; § 19, 4.). Diese Zahl s hängt daher nur von den beiden Klassen A, C ab und kann füglich mit (A, C) bezeichnet werden. Der Wert des Symbols (A, C) ist gleich 0 zu setzen, wenn C nicht durch A teilbar ist. Die Dimension einer Klasse A wird hiernach mit (O, A) bezeichnet, wo O die aus dem Nulleck $\mathfrak{O}$ bestehende Klasse bedeutet. Ist (nach § 18, 8.)

$$C = AB,$$

so folgt:

$$(1) \qquad (A, C) = (A, AB) = (O, B);$$

denn die Polygone $\mathfrak{B}_1, \mathfrak{B}_2, \ldots \mathfrak{B}_s$, die sämtlich in B enthalten sind, sind linear unabhängig, daher (O, B) gewiß nicht kleiner als s. Ist umgekehrt $\mathfrak{B}$ ein beliebiges Polygon der Klasse B, so ist $\mathfrak{A}\mathfrak{B}$ in C

enthalten, also auch in der Schar $(\mathfrak{A}\mathfrak{B}_1, \mathfrak{A}\mathfrak{B}_2, \ldots \mathfrak{A}\mathfrak{B}_s)$, mithin $\mathfrak{B}$ in der Schar $(\mathfrak{B}_1, \mathfrak{B}_2, \ldots \mathfrak{B}_s)$ enthalten, d. h. $(O, B) = s$.

Ist a die Ordnung der Klasse A, so ist nach § 20, 2.

$$(A, B) \leqq (O, C) - a,$$

und daraus folgt mittels (1) der allgemeine Satz

$$(2) \qquad (O, B) \leqq (O, AB) - a.$$

3. Haben die sämtlichen Basis-Polygone einer Klasse A den größten gemeinschaftlichen Teiler $\mathfrak{M}$, so ist dieser auch Teiler sämtlicher Polygone der Klasse A. Ist $\mathfrak{M}$ gleich dem Nulleck $\mathfrak{O}$, so heißt die Klasse eine eigentliche, im entgegengesetzten Falle eine uneigentliche vom Teiler $\mathfrak{M}$.

Unterdrückt man in sämtlichen Polygonen einer uneigentlichen Klasse A den Teiler $\mathfrak{M}$, so erhält man eine eigentliche Klasse A' von niedrigerer Ordnung, aber von derselben Dimension. Diese Beziehung von A zu A' soll durch das Zeichen ausgedrückt sein

$$A = \mathfrak{M} A'.$$

4. Der Teiler $\mathfrak{M}$ einer uneigentlichen Klasse A ist stets ein isoliertes Polygon. Ist nämlich

$$A = \mathfrak{M} A',$$

so kann man in der eigentlichen Klasse A' nach § 19, 2. ein Polygon $\mathfrak{A}'$ so wählen, daß es relativ prim zu $\mathfrak{M}$ ist. Ist also $\mathfrak{M}'$ äquivalent mit $\mathfrak{M}$, so ist $\mathfrak{M}'\mathfrak{A}'$ äquivalent $\mathfrak{M}\mathfrak{A}'$, also in A enthalten, mithin durch $\mathfrak{M}$ teilbar. Es ist also auch $\mathfrak{M}'$ durch $\mathfrak{M}$ teilbar, und da $\mathfrak{M}$ und $\mathfrak{M}'$ von gleicher Ordnung sind,

$$\mathfrak{M} = \mathfrak{M}'.$$

Hiernach bildet das einzige Polygon $\mathfrak{M}$ eine Klasse $\boldsymbol{M}$, und die Bezeichnung $\mathfrak{M}A'$ ist gleichbedeutend mit $\boldsymbol{M}A'$ (§ 18, 6.).

§ 22.

Die Normalbasen von $\mathfrak{o}$.

1. Wir betrachten im folgenden das System $\mathfrak{o}$ der ganzen Funktionen ω einer beliebigen Variablen z in Ω und zugleich das System $\mathfrak{o}'$ der ganzen Funktionen ω' von $z' = \frac{1}{z}$. Aus der Definition der ganzen Funktionen erhellt sofort, daß die beiden Systeme $\mathfrak{o}$, $\mathfrak{o}'$ nur die Konstanten miteinander gemein haben, daß dagegen jede Funktion ω

durch Multiplikation mit einer bestimmten positiven Potenz von z' in eine Funktion ω' verwandelt werden kann. Ist $\omega z'^r$ in $\mathfrak{o}'$ enthalten, so gilt das gleiche auch von $\omega z'^{r+1}$, $\omega z'^{r+2}$, ... In der Reihe der Funktionen

$$\omega, \quad \frac{\omega}{z} = z'\omega, \quad \frac{\omega}{z^2} = z'^2\omega, \ldots$$

werden also von einem bestimmten Gliede $\omega z'^r$ an alle folgenden Funktionen in $\mathfrak{o}'$ enthalten sein, während alle vorangehenden nicht darin enthalten sind. Die kleinste Zahl r, für welche $z'^r\omega$ in $\mathfrak{o}'$ enthalten ist, soll der **Exponent** der Funktion ω in bezug auf z genannt werden. Die Konstanten, und nur diese, haben den Exponenten Null. Ist ω von Null verschieden, und r sein Exponent, so ist $r+1$ der Exponent von $(z-c)\omega$; denn ist $\omega = z'^r\omega'$, so ist

$$\frac{(z-c)\omega}{z^{r+1}} = (1-cz')\omega' \quad \text{in } \mathfrak{o}' \text{ enthalten,}$$

$$\frac{(z-c)\omega}{z^r} = z\omega' - c\omega' \quad \text{nicht in } \mathfrak{o}' \text{ enthalten,}$$

da zwar $c\omega'$, nicht aber $z\omega' = \frac{\omega}{z^{r-1}}$ in $\mathfrak{o}'$ enthalten ist. Daraus folgt allgemein:

Ist x eine ganze rationale Funktion von z vom Grade s, und r der Exponent von ω, so ist $(r+s)$ der Exponent von $x\omega$.

2. Wir wählen nun ein Funktionensystem $\lambda_1, \lambda_2, \ldots \lambda_n$ in $\mathfrak{o}$ nach folgender Regel aus:

Es sei λ_1 eine von Null verschiedene Konstante, z. B. 1; λ_2 sei unter denjenigen Funktionen in $\mathfrak{o}$, welche nicht einer Konstanten nach dem Modul $\mathfrak{o}z$ kongruent sind, eine von möglichst niedrigem Exponenten r_2 usf.; allgemein sei λ_s unter denjenigen Funktionen in $\mathfrak{o}$, welche nicht kongruent sind einer Funktion der Schar $(\lambda_1, \lambda_2, \ldots \lambda_{s-1})$ (mod. $\mathfrak{o}z$), eine von möglichst niedrigem Exponenten r_s. Da $(\mathfrak{o}, \mathfrak{o}z) = N(z) = z^n$ vom n^{ten} Grade ist, so gibt es in $\mathfrak{o}$ n und nicht mehr nach dem Modul $\mathfrak{o}z$ linear unabhängige Funktionen (§ 6), und daher kann die Reihe der Funktionen $\lambda_1, \lambda_2, \lambda_3, \ldots$ nicht mehr und nicht weniger als n Glieder enthalten. Es ist dann (§ 5)

$$\mathfrak{o} \equiv (\lambda_1, \lambda_2, \ldots \lambda_n) \text{ (mod. } \mathfrak{o}z).$$

Die Exponenten $r_1, r_2, \ldots r_n$ der Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ genügen der Forderung

$$r_1 = 0, \quad 1 \leqq r_2 \leqq r_3 \ldots \leqq r_n.$$

Jede Funktion in $\mathfrak{o}$, deren Exponent $< r_s$, ist nach dem Modul $\mathfrak{o}z$ kongruent einer Funktion aus der $(s-1)$-fachen Schar

$$(\lambda_1, \lambda_2, \ldots \lambda_{s-1}).$$

Diese Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ bilden eine Basis von $\mathfrak{o}$, wie sich aus folgender Betrachtung ergibt.

Wäre es nicht der Fall, so könnte man (§ 3, 7.) eine lineare Funktion $z - c$ und ein System nicht alle verschwindender Konstanten $a_1, a_2, \ldots a_n$ so bestimmen, daß

$$a_1\lambda_1 + a_2\lambda_2 + \cdots + a_n\lambda_n = (z-c)\omega$$

wäre. Ist unter den Konstanten a die letzte nicht verschwindende a_s, so ist auch

$$a_1\lambda_1 + a_2\lambda_2 + \cdots + a_s\lambda_s = (z-c)\omega,$$

und der Exponent von ω ist sicher kleiner als r_s (weil $\frac{(z-c)\omega}{z^{r_s}}$ in $\mathfrak{o}'$ enthalten ist). Es ist also ω, und mithin, da a_s von 0 verschieden ist, auch λ_s kongruent einer Funktion der Schar $(\lambda_1, \lambda_2, \ldots \lambda_{s-1})$ (mod. $\mathfrak{o}z$), was gegen die Voraussetzung ist.

Die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ bilden daher eine Basis von $\mathfrak{o}$, und diese soll Normalbasis genannt werden. Die charakteristischen Eigenschaften der Normalbasis sind:

I. Die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ sind linear unabhängig nach dem Modul $\mathfrak{o}z$.

II. Jede Funktion in $\mathfrak{o}$, deren Exponent kleiner ist als der Exponent r_s von λ_s, ist in der Form enthalten

$$c_1\lambda_1 + c_2\lambda_2 + \cdots + c_{s-1}\lambda_{s-1} + z\omega_s,$$

worin $c_1, c_2, \ldots c_{s-1}$ Konstanten, ω_s eine Funktion in $\mathfrak{o}$.

3. Die in $\mathfrak{o}'$ erhaltenen Funktionen

$$\lambda_1' = \frac{\lambda_1}{z^{r_1}}, \quad \lambda_2' = \frac{\lambda_2}{z^{r_2}}, \quad \cdots \quad \lambda_n' = \frac{\lambda_n}{z^{r_n}}$$

bilden eine Normalbasis von $\mathfrak{o}'$.

Ist nämlich ω eine durch z nicht teilbare Funktion in $\mathfrak{o}$ vom Exponenten r, so ist der Exponent von $\omega' = \frac{\omega}{z^r}$ in bezug auf z' ebenfalls r; denn es ist zwar $\frac{\omega'}{z'^r} = \omega$, aber nicht $\frac{\omega'}{z'^{r-1}} = \frac{\omega}{z}$ in $\mathfrak{o}$ enthalten. Da die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ alle durch z nicht teilbar sind, so sind hiernach die Exponenten von $\lambda_1', \lambda_2', \ldots \lambda_n'$ in bezug auf z'

resp. $r_1, r_2, \ldots r_n$. Dies vorausgeschickt beweisen wir, daß das Funktionensystem $\lambda_1', \lambda_2', \ldots \lambda_n'$ die Eigenschaften I., II. besitzt, wenn dort o, z durch o', z' ersetzt werden.

Wäre die Bedingung I. nicht erfüllt, so ließen sich die Konstanten $a_1, a_2, \ldots a_s$, deren letzte nicht verschwindet, so bestimmen, daß

$$a_1 \lambda_1' + a_2 \lambda_2' + \cdots + a_s \lambda_s' = z' \omega',$$

also auch (durch Multiplikation mit z^{r_s})

$$a_1 z^{r_s - r_1} \lambda_1 + a_2 z^{r_s - r_2} \lambda_2 + \cdots + a_s \lambda_s = \omega,$$

worin

$$\omega = z^{r_s - 1} \omega',$$

also eine Funktion in o, deren Exponent kleiner als r_s wäre. Dies ist aber, da a_s von Null verschieden, wegen der Voraussetzung über die λ unmöglich, und folglich die Bedingung I. erfüllt; daraus folgt:

$$o' \equiv (\lambda_1', \lambda_2', \ldots \lambda_n') \text{ (mod. } o' z').$$

Wäre die Bedingung II. nicht erfüllt, und λ' eine Funktion in o', deren Exponent $r < r_s$, die nicht in der Form enthalten ist

$$a_1 \lambda_1' + a_2 \lambda_2' + \cdots + a_{s-1} \lambda_{s-1}' + z' \omega',$$

so könnte man $e \gtreqless s$ so wählen, daß

$$\lambda' = a_1 \lambda_1' + a_2 \lambda_2' + \cdots + a_e \lambda_e' + z' \omega'$$

mit konstanten Koeffizienten, deren letzter a_e nicht verschwindet. Es ist hiernach auch $r_e \gtreqless r_s > r$.

Demnach ist $\lambda = z^{r_e - 1} \lambda'$ eine Funktion in o, und es ergibt sich durch Multiplikation mit z^{r_e}

$$z \lambda = a_1 z^{r_e - r_1} \lambda_1 + a_2 z^{r_e - r_2} \lambda_2 + \cdots + a_e \lambda_e + z^{r_e - 1} \omega'.$$

Es ist daher $\omega = z^{r_e - 1} \omega'$ eine Funktion in o, deren Exponent (nach 1.) $\lesseqgtr r_e - 1$, und welche der Kongruenz genügt

$$\omega \equiv a_1' \lambda_1 + a_2' \lambda_2 + \cdots + a_e' \lambda_e \text{ (mod. } o z),$$

worin $a_e' = -a_e$ von Null verschieden ist. Hiernach müßte aber wegen der Eigenschaft II. der Funktionen λ der Exponent von $\omega \gtreqless r_e$ sein, woraus der Widerspruch erhellt.

Hiermit ist nachgewiesen, daß das Funktionensystem $\lambda_1', \lambda_2' \ldots \lambda_n'$ eine Normalbasis von o' bildet.

4. Wir bilden nun die Diskriminante von Ω in bezug auf die Variable z und z' mit Hilfe der beiden Normalbasen λ, λ'; es ist:

$$\Delta_z (\Omega) = \text{konst. } \Delta(\lambda_1, \lambda_2, \ldots \lambda_n),$$

$$\Delta_{z'} (\Omega) = \text{konst. } \Delta(\lambda_1', \lambda_2', \ldots \lambda_n').$$

Setzt man aber für λ_i' die Ausdrücke $z'^{r_i}\lambda_i$, so folgt aus dem Satze § 2, (13)

$$\Delta_{z'}(\Omega) = \text{konst. } z'^{2(r_1+r_2+\cdots+r_n)}\,\Delta_z(\Omega).$$

Ist $\Delta_z(\Omega)$ vom Grade δ, so besitzt $\Delta_{z'}(\Omega)$ die Wurzel $z'=0$ $[2(r_1+r_2+\cdots+r_n)-\delta]$-mal, und daraus ergibt sich nach § 16, 2. die Verzweigungszahl

$$w_z = 2(r_1+r_2+\cdots+r_n),$$

welche hiernach stets eine gerade Zahl ist.

§ 23.

Die Differentialquotienten.

1. Da eine jede von Null verschiedene Funktion des Körpers Ω nur in einer endlichen Anzahl von Punkten den Wert Null hat, so folgt, daß eine Funktion in Ω, von der sich unendlich viele Nullpunkte nachweisen lassen, notwendig identisch Null ist, oder daß zwei Funktionen in Ω, welche in unendlich vielen Punkten denselben Wert haben, identisch sein müssen.

2. Sind α, β irgend zwei Variable des Körpers Ω, so existiert in Ω eine mit $\left(\frac{d\alpha}{d\beta}\right)$ zu bezeichnende Funktion, welche in unendlich vielen Punkten $\mathfrak{P}$ der Bedingung genügt:

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0,$$

welche der Differentialquotient von α nach β genannt wird. Ist nämlich $F(\alpha,\beta)=0$ die zwischen α, β bestehende irreduktible Gleichung, so ist, wenn wir zunächst diejenigen (in endlicher Zahl vorhandenen) Punkte ausschließen, in welchen α_0 oder $\beta_0=\infty$ oder $F'(\alpha_0)=0$ oder $F'(\beta_0)=0$ ist,

$$\begin{aligned}0 = F(\alpha,\beta) &= F(\alpha_0,\beta_0)+(\alpha-\alpha_0)F'(\alpha_0)+(\beta-\beta_0)F'(\beta_0)\\ &+\tfrac{1}{2}\{(\alpha-\alpha_0)^2F''(\alpha_0,\alpha_0)+2(\alpha-\alpha_0)(\beta-\beta_0)F''(\alpha_0,\beta_0)\\ &+(\beta-\beta_0)^2F''(\beta_0,\beta_0)\}+\cdots\end{aligned}$$

Von den beiden Quotienten $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$, $\left(\frac{\beta-\beta_0}{\alpha-\alpha_0}\right)_0$ ist gewiß der eine

endlich; ist es der erstere, so ziehen wir aus der letzten Gleichung die folgende:

$$0 = \frac{\alpha-\alpha_0}{\beta-\beta_0} F'(\alpha_0) + F'(\beta_0)$$
$$+ (\beta-\beta_0)\frac{1}{2}\left\{\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)^2 F''(\alpha_0,\alpha_0) + 2\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right) F''(\alpha_0,\beta_0) + F''(\beta_0,\beta_0)\right\} + \cdots,$$

woraus für den Punkt $\mathfrak{P}$ folgt:

$$\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0 = -\frac{F'(\beta_0)}{F'(\alpha_0)} = -\left(\frac{F'(\beta)}{F'(\alpha)}\right)_0.$$

Wäre $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$ unendlich, so würden wir ebenso in bezug auf $\frac{\beta-\beta_0}{\alpha-\alpha_0}$ schließen.

Es hat also

$$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)} \tag{1}$$

die verlangte Eigenschaft. Dies bleibt auch noch richtig, wenn von den beiden Funktionen α, β eine konstant ist; denn ist z. B. α konstant, so ist $F(\alpha,\beta) = \alpha - \alpha_0$ von β unabhängig, also $F'(\alpha) = 1$, $F'(\beta) = 0$.

3. Aus vorstehendem folgt, daß, falls β nicht konstant ist, abgesehen von einer endlichen Anzahl von Punkten $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$ ein endlicher Wert ist. Ist daher γ eine dritte Variable in $\mathfrak{Q}$, so ist in unendlich vielen Punkten

$$\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0 = \left(\frac{\alpha-\alpha_0}{\gamma-\gamma_0}\right)_0 \left(\frac{\gamma-\gamma_0}{\beta-\beta_0}\right)_0,$$

also auch

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{d\alpha}{d\gamma}\right)_0 \left(\frac{d\gamma}{d\beta}\right)_0.$$

Hiernach und nach 1. ist aber die Identität erfüllt:

$$\left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right)\left(\frac{d\gamma}{d\beta}\right)^{*}). \tag{2}$$

*) Man kann auch den Differentialquotienten durch die Gleichung

$$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)}$$

definieren und durch algebraische Division zum Beweis des Satzes

$$\left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right)\left(\frac{d\gamma}{d\beta}\right)$$

gelangen.

4. Infolge dieses letzten Satzes können wir jeder der Funktionen $\alpha, \beta, \gamma, \ldots$ des Körpers Ω eine Funktion $d\alpha, d\beta, d\gamma, \ldots$ (Differential) in der Weise zuordnen, daß allgemein

$$\frac{d\alpha}{d\beta} = \left(\frac{d\alpha}{d\beta}\right)$$

wird. Die Differentiale der Konstanten, und nur diese sind Null zu setzen; die übrigen sind völlig bestimmt, sobald eines derselben willkürlich angenommen ist. Besteht zwischen den Variablen $\alpha, \beta, \gamma, \ldots$ eine rationale Gleichung

$$F(\alpha, \beta, \gamma, \ldots) = 0,$$

so folgt aus derselben

$$F'(\alpha)d\alpha + F'(\beta)d\beta + F'(\gamma)d\gamma + \cdots = 0; \tag{3}$$

denn auf dieselbe Weise wie in 2. schließt man, daß diese Gleichung für unendlich viele Punkte befriedigt ist.

Unmittelbare Folgen des letzten Satzes sind die bekannten Regeln für die Differentiation von Summen, Differenzen, Produkten und Quotienten:

$$d(\alpha \pm \beta) = d\alpha \pm d\beta, \tag{4}$$

$$d(\alpha\beta) = \alpha d\beta + \beta d\alpha, \tag{5}$$

$$d\left(\frac{\alpha}{\beta}\right) = \frac{\beta d\alpha - \alpha d\beta}{\beta^2}. \tag{6}$$

5. Ist ω eine ganze Funktion von z, so wird im allgemeinen $\frac{d\omega}{dz}$ keine ganze Funktion von z sein. Es ist aber aus dem Ausdruck (§ 3, 7.)

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

ersichtlich, da die Differentialquotienten der ganzen rationalen Funktionen $x_1, x_2, \ldots x_n$ wieder ganze rationale Funktionen sind, daß die Unterideale der sämtlichen Funktionen $\frac{d\omega}{dz}$ in einem bestimmten Ideal aufgehen müssen, nämlich in dem kleinsten gemeinschaftlichen Vielfachen der Unterideale von $\frac{d\omega_1}{dz}, \frac{d\omega_2}{dz}, \ldots \frac{d\omega_n}{dz}$. Es soll untersucht werden, welches dies Ideal ist. Zu dem Ende sei $z - c$ eine beliebige lineare Funktion von z und

$$\mathfrak{o}(z-c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots,$$

worin die Primideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... voneinander verschieden sind. Es sei nun ζ dieselbe Funktion wie in § 11, 2., d. h. eine ganze Funktion von z, welche in den durch die Primideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... erzeugten Punkten $\mathfrak{P}$, $\mathfrak{P}_1$, $\mathfrak{P}_2$, ... lauter verschiedene Werte hat und jeden derselben nur einfach; dann läßt sich ω in der Form darstellen

$$\omega = y_0 + y_1\zeta + \cdots + y_{n-1}\zeta^{n-1},$$

worin die rationalen Funktionen y_0, y_1, ... y_{n-1} von z zwar gebrochen sein können, aber den Faktor $z-c$ gewiß nicht im Nenner enthalten. Daraus folgt, daß das Unterideal von $\frac{d\omega}{dz}$ durch keine höheren Potenzen der Ideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... teilbar sein kann, als das Unterideal von $\frac{d\zeta}{dz}$. Ist aber

$$f(\zeta, z) = 0$$

die zwischen ζ und z bestehende irreduktible Gleichung, so ist nach § 11, 2.

$$\mathfrak{o} f'(\zeta) = \mathfrak{m}\mathfrak{p}^{e-1}\mathfrak{p}_1^{e_1-1}\mathfrak{p}_2^{e_2-1}\ldots$$

und $\mathfrak{m}$ relativ prim zu $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... Da aber

$$\frac{d\zeta}{dz} = -\frac{f'(z)}{f'(\zeta)}$$

ist, so kann das Unterideal von $\frac{d\zeta}{dz}$, und mithin auch das von $\frac{d\omega}{dz}$ keinen der Faktoren $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... öfter als $(e-1), (e_1-1), (e_2-1), \ldots$-mal enthalten. Da nun $z-c$ jede beliebige lineare Funktion sein kann, so folgt, daß $\frac{d\omega}{dz}$ kein anderes Unterideal haben kann, als ein solches, welches in dem Verzweigungsideal $\mathfrak{z} = \Pi\mathfrak{p}^{e-1}$ (§ 11) aufgeht. Es ist also, wenn $\mathfrak{a}$ ein Ideal bedeutet:

$$\mathfrak{z}\frac{d\omega}{dz} = \mathfrak{a},$$

also nach § 11, (7)

$$\mathfrak{o}\frac{d\omega}{dz} = \mathfrak{e}\mathfrak{a},$$

woraus hervorgeht, daß die Funktionen $\frac{d\omega}{dz}$ sämtlich dem zu $\mathfrak{o}$ komplementären Modul $\mathfrak{e}$ angehören.

6. Ist die irreduktible Gleichung $F(\omega, z) = 0$ zwischen ω und z vom n^{ten} Grade in bezug auf ω, also $1, \omega, \omega^2, \ldots \omega^{n-1}$ eine Basis von $\mathfrak{Q}$. so ist nach § 11, (10)

$$\mathfrak{o}F'(\omega) = \mathfrak{d}\mathfrak{k},$$

und daher muß wegen

$$\frac{d\omega}{dz} = -\frac{F'(z)}{F'(\omega)}$$

$\mathfrak{o}F'(z)$ durch das Ideal $\mathfrak{k}$ teilbar sein,

$$\mathfrak{o}F'(z) = \mathfrak{k}\mathfrak{a},$$

$\mathfrak{k}$ kann man daher das Ideal der Doppelpunkte in bezug auf ω, z nennen.

7. Ist $\mathfrak{P}$ ein Punkt, in welchem $z - c$ unendlich klein in der ersten Ordnung ist (also kein Verzweigungspunkt in z), so sind nach 5. die Funktionen $\frac{d\omega}{dz}$ in $\mathfrak{P}$ alle endlich. Ist also η irgendeine Funktion in $\mathfrak{Q}$, welche in $\mathfrak{P}$ endlich ist, so kann man diese als Quotienten zweier ganzen Funktionen $\frac{\alpha}{\beta}$ darstellen, von denen β in $\mathfrak{P}$ nicht verschwindet, und daher ist nach (6) auch $\frac{d\eta}{dz}$ in $\mathfrak{P}$ endlich

8. Es seien jetzt α, β irgend zwei Variable in $\mathfrak{Q}$; es soll das Verhalten von $\frac{d\alpha}{d\beta}$ in irgendeinem Punkte $\mathfrak{P}$ untersucht werden.

Man wähle eine Variable z in $\mathfrak{Q}$, welche in $\mathfrak{P}$ unendlich klein in der ersten Ordnung ist. Hat α in $\mathfrak{P}$ einen endlichen Wert α_0, so kann man nach § 15, 1., 2. eine positive ganze Zahl r und eine in $\mathfrak{P}$ endliche und von Null verschiedene Funktion α' so bestimmen, daß

$$\alpha = \alpha_0 + z^r\alpha'$$

wird. Dies gilt auch noch, wenn α in $\mathfrak{P}$ unendlich ist; nur ist dann r eine negative ganze Zahl, und α_0 ist durch eine beliebige endliche Konstante, z. B. 0 zu ersetzen. Ebenso kann man

$$\beta = \beta_0 + z^s\beta'$$

setzen; r und s sind dann die Ordnungszahlen von $\alpha - \alpha_0$, $\beta - \beta_0$ im Punkte $\mathfrak{P}$, die sowohl positiv als negativ, aber nicht 0 sein können. Aus (2) ergibt sich dann:

$$\frac{d\alpha}{d\beta} = z^{r-s}\frac{r\alpha' + z\frac{d\alpha'}{dz}}{s\beta' + z\frac{d\beta'}{dz}}$$

oder

$$\frac{\beta-\beta_0}{\alpha-\alpha_0}\frac{d\alpha}{d\beta}=\frac{r+z\dfrac{d\alpha'}{\alpha' dz}}{s+z\dfrac{d\beta'}{\beta' dz}}.$$

Bezeichnet man nun wieder durch den Index 0 den Wert einer Funktion im Punkte $\mathfrak{P}$, so ist, da

$$\left(\frac{d\alpha'}{\alpha' dz}\right)_0,\quad \left(\frac{d\beta'}{\beta' dz}\right)_0$$

nach 7. endlich sind,

$$\left(\frac{\beta-\beta_0}{\alpha-\alpha_0}\frac{d\alpha}{d\beta}\right)_0=\frac{r}{s}, \tag{7}$$

also endlich und von Null verschieden. Hieraus ergibt sich, daß die Ordnungszahl des Differentialquotienten $\frac{d\alpha}{d\beta}$ gleich ist der Differenz der Ordnungszahlen von $\alpha-\alpha_0$ und $\beta-\beta_0$. Ist $r\gtrless s$, so ist $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$ und mithin $\left(\frac{d\alpha}{d\beta}\right)_0$ Null oder unendlich. Ist dagegen $r=s$, so sind beide Werte endlich und von 0 verschieden, und wir haben daher in allen Fällen

$$\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0=\left(\frac{d\alpha}{d\beta}\right)_0. \tag{8}$$

Hierin sind α_0, β_0 die Werte von α, β in $\mathfrak{P}$, wenn diese Werte endlich sind, sonst beliebige Konstanten, z. B. 0.

9. Sind a, b die Ordnungszahlen von $\alpha-\alpha_0$, $\beta-\beta_0$ in $\mathfrak{P}$, so kommt, falls a, b positiv sind, der Punkt $\mathfrak{P}$ $(a-1)$-mal resp. $(b-1)$-mal in den Verzweigungspolygonen $\mathfrak{Z}_\alpha$, $\mathfrak{Z}_\beta$ in α, β vor. Ist aber a negativ, so enthält $\mathfrak{Z}_\alpha$ den Punkt $\mathfrak{P}$ $(-a-1)$-mal, und Entsprechendes gilt, wenn b negativ ist (§ 16, 1.). Bezeichnet man also mit $\mathfrak{A}$, $\mathfrak{B}$ die Unterecke von α, β, so erhält man, weil die Ordnungszahl von $\frac{d\alpha}{d\beta}$ (wie eben bewiesen) immer gleich $a-b$ ist, für diese Funktion folgenden Ausdruck als Polygonquotienten

$$\frac{d\alpha}{d\beta}=\frac{\mathfrak{Z}_\alpha\mathfrak{B}^b}{\mathfrak{Z}_\beta\mathfrak{A}^a}. \tag{9}$$

§ 24.

Das Geschlecht des Körpers Ω.

1. Bezeichnet man mit w_α, w_β die Verzweigungszahlen, mit n_α, n_β die Ordnungen der Variablen α, β, so folgt aus der Formel (9) des vorigen §, da Zähler und Nenner von $\frac{d\alpha}{d\beta}$ gleichviel Punkte enthalten müssen, die wichtige Relation

$$w_\alpha - 2n_\alpha = w_\beta - 2n_\beta;$$

wenn man also

$$p = \tfrac{1}{2}w - n + 1 \tag{1}$$

setzt, welches nach § 22, 4. eine ganze Zahl ist, so ist diese von der Wahl der Variablen unabhängig und eine für den Körper Ω charakteristische Zahl, welche das Geschlecht des Körpers Ω genannt wird. Daß diese Zahl niemals negativ ist, ergibt sich, wenn man für $\frac{1}{2}w$ den Wert $r_1 + r_2 + \cdots + r_n$ aus § 22 einsetzt. Man erhält dann

$$p = (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1), \tag{2}$$

was, da $r_2, r_3, \ldots r_n \geqq 1$ sind, nicht negativ werden kann.

2. Es seien α, β zwei Funktionen in Ω von den Ordnungen m, n, von der Beschaffenheit, daß alle Funktionen in Ω rational durch α, β darstellbar sind. Es ist dann

$$\begin{aligned} F(\alpha, \beta) &= a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n \\ &= b_0\beta^m + b_1\beta^{m-1} + \cdots + b_{m-1}\beta + b_m = 0 \end{aligned}$$

die zwischen α, β bestehende irreduktible Gleichung, worin $a_0, a_1, \ldots a_n$ ganze rationale Funktionen von β, ebenso $b_0, b_1, \ldots b_m$ ganze rationale Funktionen von α sind.

Es sei ferner

$$\alpha = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \beta = \frac{\mathfrak{B}_1}{\mathfrak{B}}$$

und $\mathfrak{A}_1$ relativ prim zu $\mathfrak{A}$, $\mathfrak{B}_1$ zu $\mathfrak{B}$, so daß $\mathfrak{A}$, $\mathfrak{A}_1$ von der Ordnung m, $\mathfrak{B}$, $\mathfrak{B}_1$ von der Ordnung n sind. Nun ist

$$\begin{aligned} F'(\alpha) &= n a_0 \alpha^{n-1} + (n-1) a_1 \alpha^{n-2} + \cdots + a_{n-1}, \\ \alpha F'(\alpha) &= -a_1\alpha^{n-1} - 2a_2\alpha^{n-2} - \cdots - n a_n, \end{aligned}$$

woraus hervorgeht, daß

$$F'(\alpha) = \frac{\mathfrak{R}}{\mathfrak{A}^{n-1}\mathfrak{B}^m}$$

und ebenso

$$F'(\beta) = \frac{\mathfrak{L}}{\mathfrak{A}^n \mathfrak{B}^{m-2}}$$

sein muß. Es ist nun nachzuweisen, daß das Polygon $\mathfrak{K}$ durch $\mathfrak{Z}_\beta$, $\mathfrak{L}$ durch $\mathfrak{Z}_\alpha$ teilbar ist.

Für $\mathfrak{K}$ ist dies leicht einzusehen unter der Voraussetzung, daß in sämtlichen Punkten von $\mathfrak{Z}_\beta$ die Funktion β einen endlichen, und a_0 einen von Null verschiedenen Wert hat; denn es ist

$$\alpha' = a_0 \alpha$$

eine ganze Funktion von β, und wenn man

$$f(\alpha') = a^{n-1} F(\alpha, \beta)$$

setzt, so ist

$$f'(\alpha') = a_0^{n-2} F'(\alpha).$$

Da nun nach § 11, 5. $\mathfrak{v}_\beta f'(\alpha')$ durch das von $\mathfrak{Z}_\beta$ erzeugte Verzweigungsideal in β teilbar ist, so folgt hieraus die Richtigkeit der Behauptung. Analoges gilt für $F'(\beta)$.

Macht man nun für α, β beliebige lineare Substitutionen:

$$\alpha = \frac{c + d\alpha'}{a + b\alpha'}; \quad \beta = \frac{c' + d'\beta'}{a' + b'\beta'},$$

$$(a + b\alpha')(d - b\alpha) = ad - bc,$$

$$(a' + b'\beta')(d' - b'\beta) = a'd' - b'c',$$

so ist nach § 16, 2.

$$\mathfrak{Z}_\alpha = \mathfrak{Z}_{\alpha'}; \quad \mathfrak{Z}_\beta = \mathfrak{Z}_{\beta'},$$

und die zwischen α', β' bestehende irreduktible Gleichung lautet:

$$F_1(\alpha', \beta') = (a + b\alpha')^n (a' + b'\beta')^m F(\alpha, \beta) = 0.$$

Es lassen sich aber unter allen Umständen die Konstanten a, b, c, d; a', b', c', d' so wählen, daß die oben angegebenen Voraussetzungen sowohl für α' als für β' erfüllt sind.

Denn setzt man die Koeffizienten a'_0, b'_0 von α'^n, β'^m in $F_1(\alpha', \beta')$ in die Form

$$a'_0 = (a' + b'\beta')^m (a^0 d^n + a_1 d^{n-1} b + \cdots + a_n b^n)$$

$$= \left(\frac{a'd' - b'c'}{d' - b'\beta}\right)^m (a_0 d^n + a_1 d^{n-1} b + \cdots + a_n b^n),$$

$$b'_0 = (a + b\alpha')^n (b_0 d'^m + b_1 d'^{m-1} b' + \cdots + b_m b'^m)$$

$$= \left(\frac{ad - bc}{d - b\alpha}\right)^n (b_0 d'^m + b_1 d'^{m-1} b' + \cdots + b_m b'^m),$$

so erkennt man leicht, daß nur für eine endliche Anzahl von Werten der Verhältnisse $d:b$, $d':b'$ die Funktionen a'_0, $d'-b'\beta$ in einem Punkte von $\mathfrak{Z}_\beta$, $b'_0, d-b\alpha$ in einem Punkte von $\mathfrak{Z}_\alpha$ verschwinden können.

Setzen wir nun

$$\alpha' = \frac{\mathfrak{A}'_1}{\mathfrak{A}'}, \quad \beta' = \frac{\mathfrak{B}'_1}{\mathfrak{B}'},$$

so folgt (§ 19, 1.)

$$d-b\alpha = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad a+b\alpha' = \frac{\mathfrak{A}'_2}{\mathfrak{A}'},$$

also:

$$\mathfrak{A}_2\mathfrak{A}'_2 = \mathfrak{A}\mathfrak{A}'.$$

Ist aber, wie angenommen, b von Null verschieden, so ist $\mathfrak{A}_2$ relativ prim zu $\mathfrak{A}$, weil in einem Punkte von $\mathfrak{A}$ die Ordnungszahl von $d-b\alpha$ dieselbe ist, wie die von α (§ 15, 5.) und folglich

$$\mathfrak{A}_2 = \mathfrak{A}', \quad \mathfrak{A}'_2 = \mathfrak{A},$$

also:

$$a+b\alpha' = \frac{\mathfrak{A}}{\mathfrak{A}'},$$

und ebenso:

$$a'+b'\beta' = \frac{\mathfrak{B}}{\mathfrak{B}'}.$$

Nun ist aber, da $F(\alpha, \beta) = 0$ ist:

$$F'_1(\alpha') = (ad-bc)(a+b\alpha')^{n-2}(a'+b'\beta')^m F'(\alpha),$$

und wenn also, wie vorausgesetzt:

$$F'_1(\alpha') = \frac{\mathfrak{R}\,\mathfrak{Z}_\beta}{\mathfrak{A}'^{n-2}\mathfrak{B}'^m},$$

so folgt

$$F'(\alpha) = \frac{\mathfrak{R}\,\mathfrak{Z}_\beta}{\mathfrak{A}^{n-2}\mathfrak{B}^m}$$

und in gleicher Weise

$$F'(\beta) = \frac{\mathfrak{R}\,\mathfrak{Z}_\alpha}{\mathfrak{A}^n\mathfrak{B}^{m-2}}.$$

Daß das im Zähler dieser beiden Ausdrücke auftretende Polygon $\mathfrak{R}$ in beiden Ausdrücken dasselbe sein muß, ergibt sich aus

$$\frac{d\alpha}{d\beta} = -\frac{F'(\beta)}{F'(\alpha)} = \frac{\mathfrak{B}^2\,\mathfrak{Z}_\alpha}{\mathfrak{A}^2\,\mathfrak{Z}_\beta}.$$

Nun ist die Ordnung des Polygons $\mathfrak{A}^{n-2}\mathfrak{B}^m$

$$m(n-2)+mn = 2m(n-1),$$

also die Ordnung von $\mathfrak{R}$

$$2r = 2m(n-1) - w_\beta$$

stets eine gerade Zahl, und daraus ergibt sich

(3) $$p = \tfrac{1}{2}w_\beta - n + 1 = (n-1)(m-1) - r.$$

Das Polygon $\mathfrak{R}$ wird das Polygon der Doppelpunkte in (α, β) genannt.

§ 25.

Die Differentiale in Ω.

Sind z, z_1 irgend zwei Variable in Ω von den Ordnungen n, n_1 und den Verzweigungszahlen w, w_1, ferner $\mathfrak{Z}$, $\mathfrak{Z}_1$ die Verzweigungspolygone, $\mathfrak{U}$, $\mathfrak{U}_1$ die Unterecke von z, z_1, so ist (§ 23)

(1) $$\frac{dz}{dz_1} = \frac{\mathfrak{Z}\mathfrak{U}_1^2}{\mathfrak{Z}_1\mathfrak{U}^2}.$$

Jede Funktion ω in Ω läßt sich in die Form setzen

(2) $$\omega = \frac{\mathfrak{U}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}},$$

worin $\mathfrak{A}$, $\mathfrak{B}$ Polygone bedeuten, deren Ordnungen a, b der Bedingung genügen

$$2n + a = w + b$$

oder (§ 24)

(3) $$a = b + 2p - 2.$$

Wenn man nun eine Funktion ω_1 durch die Gleichung erklärt

$$\omega\, dz = \omega_1\, dz_1,$$

so erhält nach (1) ω_1 die Bezeichnung

$$\omega_1 = \frac{\mathfrak{U}_1^2\mathfrak{A}}{\mathfrak{Z}_1\mathfrak{B}}.$$

Wir nennen in der Folge solche Ausdrücke, wie

$$\omega\, dz = \omega_1\, dz_1$$

Differentiale in Ω, und bezeichnen dieselben in symbolischer Weise durch ein Zeichen wie $d\tilde{\omega}$. Ein solches Differential ist hierdurch invariant, d. h. unabhängig von der Wahl der Veränderlichen z erklärt und ist durch die beiden Polygone $\mathfrak{A}$, $\mathfrak{B}$ vollständig bestimmt.

Wir können ohne Gefahr eines Mißverständnisses die symbolische Bezeichnung

$$d\tilde{\omega} = \frac{\mathfrak{A}}{\mathfrak{B}},$$

also beispielsweise auch

$$dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2}$$

anwenden. Diese Bezeichnung eines Differentials durch einen Polygonquotienten unterscheidet sich von der ähnlichen Bezeichnung der Funktionen in Ω (§ 17) dadurch, daß bei letzterer Zähler und Nenner von gleicher Ordnung sind, während bei den Differentialen die Ordnung des Zählers die des Nenners um $2p-2$ übertrifft. Wie bei der Bezeichnung in § 17, können auch hier gemeinschaftliche Teiler, welche $\mathfrak{A}$ und $\mathfrak{B}$ etwa enthalten, unterdrückt werden. Sind $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim, so heißt $\mathfrak{A}$ das Obereck, $\mathfrak{B}$ das Untereck des Differentials $d\tilde{\omega}$.

Unter den hier aufgestellten allgemeinen Begriff des Differentials in Ω fallen als spezielle Fälle auch die in § 23, 4. erkärten Differentiale der Funktionen des Körpers Ω. Diese nennen wir eigentliche Differentiale, während die anderen, welche nicht als Differentiale von in Ω existierenden Funktionen dargestellt werden können, uneigentliche oder Abelsche Differentiale genannt werden.

Funktionen von der Form (2), die nach unserer jetzt getroffenen Festsetzung mit $\frac{d\tilde{\omega}}{dz}$ bezeichnet werden können, nennen wir Differentialquotienten nach z und unterscheiden gleichfalls zwischen eigentlichen und uneigentlichen Differentialquotienten, je nachdem $d\tilde{\omega}$ ein eigentliches oder uneigentliches Differential ist*).

Es entsteht nun die Aufgabe, den Umfang des Begriffs der Differentiale festzustellen, d. h. alle Polygone $\mathfrak{A}$, $\mathfrak{B}$ zu finden, welche Ober- und Untereck eines Differentials sein können. Wir schicken darüber die folgenden allgemeinen Bemerkungen voraus:

---

*) Der Quotient irgend zweier eigentlichen oder uneigentlichen Differentiale $\frac{d\tilde{\omega}}{d\tilde{\omega}'}$ hat stets die Bedeutung einer bestimmten Funktion in Ω. Wir beschränken uns im folgenden aber auf die Betrachtung solcher Quotienten, bei denen wenigstens der Nenner ein eigentliches Differential ist.

Die notwendige und hinreichende Bedingung dafür, daß $\frac{\mathfrak{A}}{\mathfrak{B}}$ ein Differential sei, ist die, daß für eine beliebige Variable z

$$\frac{\mathfrak{U}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}}$$

eine Funktion in Ω ist, also daß $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$ äquivalent ist. Dies Verhältnis bleibt aber bestehen, wenn $\mathfrak{A}$, $\mathfrak{B}$ selbst durch äquivalente Polygone $\mathfrak{A}'$, $\mathfrak{B}'$ ersetzt werden. Halten wir $\mathfrak{B}$ fest, und ist $\frac{\mathfrak{A}}{\mathfrak{B}}$ ein Differential, so werden hiernach

$$\frac{\mathfrak{A}'}{\mathfrak{B}}, \quad \frac{\mathfrak{A}''}{\mathfrak{B}}, \quad \cdots$$

dann und nur dann Differentiale darstellen, wenn die Polygone $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, ... alle derselben Klasse A angehören. Bilden die Polygone $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$, ... eine Basis von A, ist also

$$A = (\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \ldots),$$

so bilden die zugehörigen Differentialquotienten in bezug auf eine beliebige Variable z, $\frac{d\tilde{\omega}_1}{dz}$, $\frac{d\tilde{\omega}_2}{dz}$, $\frac{d\tilde{\omega}_3}{dz}$, ... die Basis einer Funktionenschar von endlicher Dimension, und dementsprechend werden wir auch $d\tilde{\omega}_1$, $d\tilde{\omega}_2$, $d\tilde{\omega}_3$, ... die Basis einer Schar von Differentialen

$$(d\tilde{\omega}_1, d\tilde{\omega}_2, d\tilde{\omega}_3, \ldots)$$

von derselben Dimension nennen. Dies besagt, daß jedes Differential $d\tilde{\omega}$, dessen Untereck $\mathfrak{B}$ oder ein Teiler von $\mathfrak{B}$ ist, in der Form dargestellt werden kann

$$d\tilde{\omega} = c_1 d\tilde{\omega}_1 + c_2 d\tilde{\omega}_2 + c_3 d\tilde{\omega}_3 + \cdots$$

mit konstanten Koeffizienten c_1, c_2, c_3, ...

§ 26.

Die Differentiale erster Gattung.

Wir betrachten zunächst die einfachsten unter den Differentialen in Ω, nämlich die, deren Untereck das Nulleck $\mathfrak{O}$ ist. Solche Differentiale (deren Existenz freilich erst noch nachzuweisen ist) heißen Differentiale erster Gattung. Das Obereck $\mathfrak{W}$ eines solchen Differentials dw, dessen Ordnung $2p-2$ ist, wird als das Grundpolygon von

dw bezeichnet und heißt ein vollständiges Polygon erster Gattung, während jeder Teiler eines solchen ein Polygon erster Gattung schlechtweg genannt wird. Ist $\mathfrak{W} = \mathfrak{A}\mathfrak{B}$, so heißen $\mathfrak{A}$, $\mathfrak{B}$ Ergänzungspolygone voneinander. Ein Polygon, welches nicht Teiler eines vollständigen Polygons erster Gattung ist, also insbesondere jedes Polygon von mehr als $2p-2$ Punkten heißt ein Polygon zweiter Gattung.

1. Nach dem oben Bemerkten bilden alle vollständigen Polygone erster Gattung eine Polygonklasse W, deren Dimension zu bestimmen ist; ergibt sich diese Dimension >0, so ist damit zugleich die Existenz der Polygone erster Gattung nachgewiesen. Diese Dimension ist aber dieselbe wie die Dimension der Schar der Differentiale erster Gattung oder auch, für eine beliebige Variable z, der Schar der Differentialquotienten erster Gattung, wenn wir als Differentialquotienten erster Gattung nach z die Funktionen

$$u = \frac{dw}{dz}$$

bezeichnen. Eine solche Funktion u hat nach § 25, (2) den Ausdruck

$$u = \frac{\mathfrak{U}^2\mathfrak{W}}{\mathfrak{Z}},$$

und man erkennt leicht aus der Betrachtung der Ordnungszahlen in den verschiedenen Punkten, daß ein solcher Differentialquotient erster Gattung durch folgende beiden Eigenschaften vollkommen definiert ist:

I. In jedem Punkte $\mathfrak{P}$, in welchem z einen endlichen Wert z_0 hat, ist

$$(u(z-z_0))_0 = 0.$$

II. In einem Punkte $\mathfrak{P}$, in welchem z unendlich ist, ist

$$(zu)_0 = 0.$$

Bedeutet wie in § 11, 4.

$$r = (z-c)(z-c_1)(z-c_2)\ldots$$

das Produkt sämtlicher voneinander verschiedenen Linearfaktoren der Diskriminante $\Delta_z(\Omega)$, $\mathfrak{r}$ das Produkt sämtlicher voneinander verschiedenen in r aufgehenden Primideale, so ist die Bedingung I. vollkommen gleichbedeutend mit der, daß ru eine Funktion in $\mathfrak{r}$, oder daß u eine Funktion des zu $\mathfrak{o}$ komplementären Moduls $\mathfrak{e}$ sein muß [§ 11, 4. (6)]. Um also die Gesamtheit der Funktionen u zu er-

halten, hat man unter den Funktionen in $\mathfrak{e}$ diejenigen aufzusuchen, welche der Bedingung II. genügen.

2. Zu diesem Zwecke legen wir eine Normalbasis $\lambda_1, \lambda_2, \ldots \lambda_n$ von $\mathfrak{o}$ zugrunde (§ 22) und bezeichnen die dazu komplementäre Basis mit $\mu_1, \mu_2, \ldots \mu_n$, so daß jede der Bedingung I. genügende Funktion, also auch jeder Differentialquotient erster Gattung, in der Form enthalten ist

$$u = y_1\mu_1 + y_2\mu_2 + \cdots + y_n\mu_n, \tag{1}$$

worin $y_1, y_2, \ldots y_n$ ganze rationale Funktionen von z sind. Aus den Grundeigenschaften der komplementären Basis ergibt sich aber (§ 10, 3.)

$$y_s = S(u\lambda_s); \quad \frac{y_s}{z^{r_s-1}} = S\left(uz \cdot \frac{\lambda_s}{z^{r_s}}\right).$$

Da nun $\frac{\lambda_s}{z^{r_s}}$ in $\mathfrak{o}'$ enthalten, also für $z = \infty$ endlich ist, und uz nach II. in jedem solchen Punkte verschwindet, so folgt (§ 16, 5.), daß $\frac{y_s}{z^{r_s-1}}$ für $z = \infty$ verschwinden muß, d. h. daß die ganze rationale Funktion y_s den Grad $r_s - 2$ nicht übersteigen kann.

Es muß daher, falls $r_s < 2$ ist, y_s verschwinden, also ist unter allen Umständen (§ 22, 2.)

$$y_1 = 0; \quad S(u) = 0$$

(Abelsches Theorem für Differentiale erster Gattung) und, falls $r_s \gtreqless 2$:

$$y_s = c_0 + c_1 z + c_2 z^2 + \cdots + c_{r_s-2} z^{r_s-2}. \tag{2}$$

Es ist noch zu zeigen, daß diese Bedingungen auch hinreichend sind, d. h. daß jede Funktion von der Form (1), in welcher die y_s den Ausdruck (2) haben, der Forderung II. genügt, oder, was dasselbe ist, daß, wenn $r_s \gtreqless 2$ ist, $z^{r_s-1}\mu_s$ in allen Punkten, in welchen z unendlich wird, verschwindet. Dies ergibt sich sofort durch die Betrachtung des Systems $\mathfrak{o}'$ der ganzen Funktionen von $z' = \frac{1}{z}$, für welches nach § 22, 3. die Funktionen

$$\lambda_1' = \frac{\lambda_1}{z^{r_1}}, \quad \lambda_2' = \frac{\lambda_2}{z^{r_2}}, \quad \ldots \quad \lambda_n' = \frac{\lambda_n}{z^{r_n}}$$

eine Normalbasis bilden. Die hierzu komplementäre Basis ist nach § 10, 5.

$$\mu_1' = z^{r_1}\mu_1, \quad \mu_2' = z^{r_2}\mu_2, \quad \ldots \quad \mu_n' = z^{r_n}\mu_n,$$

und da (wegen der Eigenschaft I., auf z', μ' angewandt)

$$z'\mu_s' = 0 \quad \text{für} \quad z' = 0,$$

so folgt

$$z^{r_s-1}\mu_s = 0 \quad \text{für} \quad z = \infty,$$

w. z. b. w.

Da aber die Funktionen $z^h\mu_s$ linear unabhängig sind (wegen der rationalen Unabhängigkeit der Funktionen μ_s), so ergibt sich hieraus nach § 24, (2) der Hauptsatz:

Die Schar der Differentiale erster Gattung ist von der Dimension

$$(r_2-1)+(r_3-1)+\cdots+(r_n-1) = p,$$

und demnach ist auch p die Dimension der Klasse W der vollständigen Polygone erster Gattung.

Als Basis der Schar der Differentialquotienten erster Gattung nach z kann man die p Funktionen $z^h\mu_s$ $(h \gtreqless r_s-2)$ wählen, und die Grundpolygone $\mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p$ der zugehörigen Differentiale dw bilden eine Basis der Klasse W.

3. Wegen einer späteren Anwendung soll hier noch eine besondere Art von Differentialquotienten erster Gattung u' betrachtet werden, nämlich die, bei welchen die Bedingung II. ersetzt ist durch die dieselbe einschließende Bedingung.

III. In jedem Punkte $\mathfrak{P}$, in welchem z unendlich ist, sei

$$(z^k u')_0 = 0,$$

wo k eine gegebene positive ganze Zahl.

Die Funktionen u' lassen sich darstellen durch

$$u' = \frac{\mathfrak{U}^{k+1}\mathfrak{W}'}{\mathfrak{Z}}$$

und bilden ebenfalls eine Schar; desgleichen bilden die Polygone $\mathfrak{W}'$ eine Klasse W', deren Ordnung ist

$$\mathfrak{w} - n(k+1) = 2p-2-n(k-1).$$

Die Polygone $\mathfrak{W}'$ sind jedoch von der Wahl der Variablen z nicht unabhängig. Die Dimension der Klasse W' läßt sich nach derselben Methode bestimmen, wie die der Klasse W. Da nämlich die Bedin-

gung I. erfüllt ist, so sind Funktionen u' gleichfalls in der Form (1) enthalten; jedoch muß jetzt

$$\frac{y_s}{z^{r_s-k}} = S\left(u' z^k \frac{\lambda_s}{z^{r_s}}\right)$$

für $z = \infty$ verschwinden, und daher kann der Grad der ganzen rationalen Funktion y_s die Zahl $r_s - k - 1$ nicht übersteigen. Es verschwindet also y_s identisch, sobald $r_s < k + 1$; andernfalls ist

$$y_s = c_0 + c_1 z + \cdots + c_{r_s-k-1} z^{r_s-k-1}. \tag{3}$$

Hat umgekehrt y_s diese Form, so wird durch die Funktion

$$u' = \sum^{s} y_s \mu_s$$

der Bedingung III. genügt, denn es hat, wie in 2. bewiesen,

$$z^k(z^{r_s-k-1}\mu_s) = z^{r_s-1}\mu_s$$

für $z = \infty$ den Wert 0.

Daraus ergibt sich, daß die Dimension der Schar der Funktionen u' und folglich auch der Klasse W'

$$= \sum^{\iota} (r_\iota - k)$$

ist, wobei jedoch in der Summe nur diejenigen Glieder beizubehalten sind, die einen positiven Wert haben. Sind alle $r_\iota - k \leqq 0$, so existieren die gesuchten Funktionen überhaupt nicht.

§ 27.

Polygonklassen erster und zweiter Gattung.

Ist $\mathfrak{A}$ ein Polygon erster Gattung, so sind alle mit $\mathfrak{A}$ äquivalenten Polygone gleichfalls von der ersten Gattung. Denn wenn $\mathfrak{A}$ und $\mathfrak{B}$ Ergänzungspolygone sind und

$$\mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

so ist, wenn A, B die Klassen von $\mathfrak{A}$ und $\mathfrak{B}$ sind:

$$AB = W,$$

und, wenn $\mathfrak{A}'$ mit $\mathfrak{A}$ äquivalent ist, auch $\mathfrak{A}'\mathfrak{B} = \mathfrak{W}'$ äquivalent mit $\mathfrak{W}$ (§ 18, 5.).

Wir nennen daher solche Klassen, welche Polygone erster Gattung enthalten, **Polygonklassen erster Gattung**, die übrigen **Polygonklassen zweiter Gattung**. Die Klasse W der vollständigen Polygone

erster Gattung heißt die Hauptklasse, und zwei Klassen A, B, die der Bedingung genügen

$$AB = W,$$

Ergänzungsklassen.

Ist

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

eine Funktion in Ω, und $\mathfrak{A}'$ relativ prim zu $\mathfrak{A}$, also die Klasse A von $\mathfrak{A}$ eine eigentliche, so nennen wir η eine Funktion erster oder zweiter Gattung, je nachdem die Klasse A von der ersten oder von der zweiten Gattung ist.

Ist A eine beliebige Klasse erster Gattung und q die Anzahl der voneinander unabhängigen Polygone $\mathfrak{W}$, die durch irgendein Polygon $\mathfrak{A}$ der Klasse A teilbar sind, so ist nach § 21, 2.

$$q = (A, W) = (O, B)$$

d. h. gleich der Dimension der Ergänzungsklasse B von A. Ebenso ist (B, W) gleich der Dimension der Klasse A. Ist A eine Klasse zweiter Gattung, so ist $(A, W) = 0$. Da p die Dimension von W ist, so ist nach § 20, 2., 3. jede Klasse, deren Ordnung $\gtreqless p-1$ ist, von der ersten Gattung, und es gibt insbesondere Klassen A von der Ordnung $p-k$ derart, daß $(A, W) = (O, B) = k$ ist. Aus den gleichen Sätzen folgt, daß es Klassen von der Ordnung p gibt, welche von der zweiten Gattung sind.

§ 28.

Der Riemann-Rochsche Satz für eigentliche Klassen.

Der Riemann-Rochsche Satz, der nach seiner gewöhnlichen Ausdrucksweise die Anzahl der willkürlichen Konstanten kennen lehrt, welche eine Funktion enthält, die in einer gewissen Anzahl gegebener Punkte unendlich wird, enthält nach unserer Darstellungsweise eine Beziehung zwischen der Dimension und der Ordnung einer Klasse, resp. einer Klasse und ihrer Ergänzungsklasse. Indem wir uns zunächst auf eigentliche Klassen beschränken, schicken wir der Ableitung dieser fundamentalen Relation die folgenden Bemerkungen voraus.

1. In einer eigentlichen Klasse A kann man nach § 19, 2. stets zwei zueinander relativ prime Polygone $\mathfrak{A}$, $\mathfrak{A}'$ auswählen (eines derselben kann in der Klasse beliebig angenommen werden). Setzt man also

$$z = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

und, wenn $\mathfrak{A}''$ ein beliebiges drittes Polygon der Klasse A bedeutet:

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}''}{\mathfrak{A}'},$$

so ist nach § 17 ω eine ganze Funktion von z, $\frac{\omega}{z}$ eine ganze Funktion von $\frac{1}{z}$. Es ist daher (§ 22) der Exponent von $\omega \leqq 1$.

Ist umgekehrt ω eine ganze Funktion von z, deren Exponent $\leqq 1$ ist, so hat es die Form

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}},$$

wo $\mathfrak{A}''$ ein Polygon der Klasse A ist. Wenn nämlich

$$\omega = \frac{\mathfrak{A}_1''}{\mathfrak{A}_1}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}_1''\mathfrak{A}}{\mathfrak{A}_1\mathfrak{A}'}$$

und $\mathfrak{A}_1''$ relativ prim zu $\mathfrak{A}_1$ angenommen wird, so kann zunächst, da ω eine ganze Funktion von z sein soll, $\mathfrak{A}_1$ keinen Punkt enthalten, der nicht auch in $\mathfrak{A}$ enthalten wäre. Es kann aber auch $\mathfrak{A}_1$ keinen Punkt öfter als $\mathfrak{A}$ enthalten, weil sonst $\frac{\omega}{z}$ in einem solchen Punkte (der nicht in $\mathfrak{A}'$ vorkommen kann) unendlich, also keine ganze Funktion von $\frac{1}{z}$ wäre. Daher ist $\mathfrak{A}$ teilbar durch $\mathfrak{A}_1$, und ω kann in die Form $\frac{\mathfrak{A}''}{\mathfrak{A}}$ gesetzt werden.

2. Um also die Gesamtheit der Polygone der Klasse A zu erhalten, haben wir nur diejenigen ganzen Funktionen von z aufzusuchen, deren Exponent $\leqq 1$ ist.

Ist n die Ordnung der Klasse A, also auch die Ordnung der Variablen z, und bilden $\lambda_1, \lambda_2, \ldots \lambda_n$ eine Normalbasis von o mit den Exponenten $r_1, r_2, \ldots r_n$, darunter r_s der letzte, welcher $\leqq 1$ ist, so kann jede Funktion ω, deren Exponent $\leqq 1$ ist, nach § 22, 2. in der Form dargestellt werden

$$\omega = c_1\lambda_1 + c_2\lambda_2 + \cdots + c_s\lambda_s + z\omega_1.$$

Da der Exponent von $z\omega_1$ aber nicht größer als 1 sein kann, so muß ω_1 eine Konstante sein, und daher

$$\omega = c_1\lambda_1 + c_2\lambda_2 + \cdots + c_s\lambda_s + c_{s+1}z.$$

Umgekehrt genügt jede Funktion von dieser Form der gestellten Forderung. Es ist also $s+1$ die Dimension der Klasse A, welche hiernach, in Übereinstimmung mit § 21, 1., stets $\leqq n+1$ ist. Die obere Grenze $n+1$ kann aber nur in dem Falle $p=0$ erreicht werden und wird auch wirklich erreicht, weil in diesem Falle $r_2, r_3, \ldots r_n = 1$ sind. Daraus ergibt sich, daß ein einzelner Punkt $\mathfrak{P}$ nur, falls $p=0$ ist, zu einer eigentlichen Klasse gehören kann.

3. Wenn von den Exponenten $r_{s+1}, r_{s+2}, \ldots r_n$ einer größer als 2 ist, so ist sicher auch $r_n > 2$, und es sind nach § 26, 2., wenn $\mathfrak{Z}$ das Verzweigungspolygon in z bedeutet,

$$\mu_n = \frac{\mathfrak{A}^2\mathfrak{W}}{\mathfrak{Z}}, \quad \mu_n z = \frac{\mathfrak{A}^2\mathfrak{W}_1}{\mathfrak{Z}} = \frac{\mathfrak{A}\mathfrak{A}'\mathfrak{W}}{\mathfrak{Z}}$$

Differentialquotienten erster Gattung nach z, also

$$\mathfrak{A}\mathfrak{W}_1 = \mathfrak{A}'\mathfrak{W}$$

oder, da $\mathfrak{A}$, $\mathfrak{A}'$ relativ prim sind,

$$\mathfrak{W} = \mathfrak{A}\mathfrak{B}, \quad \mathfrak{W}_1 = \mathfrak{A}'\mathfrak{B},$$

d. h. die Klasse A ist von der ersten Gattung (z eine Variable erster Gattung). Machen wir daher zunächst die Annahme, es sei A eine Klasse zweiter Gattung, so folgt

$$r_{s+1} = 2, \quad r_{s+2} = 2, \quad \ldots \quad r_n = 2$$

und

$$p = (r_2 - 1) + \cdots + (r_s - 1) + (r_{s+1} - 1) + \cdots + (r_n - 1) = n - s.$$

Die Dimension $s+1$ der Klasse A ist daher

$$(O, A) = n - p + 1.$$

4. Machen wir zweitens die Annahme, es sei A von der ersten Gattung und wie in § 27

$$q = (A, W),$$

so existieren q linear unabhängige, durch $\mathfrak{A}$ teilbare vollständige Polygone erster Gattung, und die diesen entsprechenden Differentialquotienten erster Gattung nach z, deren es ebenfalls q und nicht mehr linear unabhängige gibt, haben den Ausdruck

$$v = \frac{\mathfrak{A}^s\mathfrak{B}}{\mathfrak{Z}},$$

worin $\mathfrak{B}$ ein Polygon von $2p-2-n$ Punkten bedeutet; die Klasse B von $\mathfrak{B}$ ist die Ergänzungsklasse von A, und daher ihre Dimension gleich q (§ 27).

Diese Funktionen v haben aber die Eigenschaft, daß in den Eckpunkten von $\mathfrak{A}$, d. h. für $z = \infty$ nicht nur zv, sondern auch

$$z^2 v = \frac{\mathfrak{A}\mathfrak{A}'^2\mathfrak{B}}{\mathfrak{Z}}$$

verschwindet, und sind hierdurch und durch die Forderung, Differentialquotienten erster Gattung zu sein, völlig bestimmt. Denn ist

$$v = \frac{\mathfrak{A}'^2\mathfrak{B}}{\mathfrak{Z}}, \quad vz^2 = \frac{\mathfrak{A}'^2\mathfrak{B}}{\mathfrak{Z}},$$

so muß, wenn $z^2 v$ in allen Punkten von $\mathfrak{A}$ verschwinden soll, $\mathfrak{B}$ durch $\mathfrak{A}$ teilbar sein, da $\mathfrak{A}'$ relativ prim zu $\mathfrak{A}$ vorausgesetzt ist. Es ist daher nach § 26, 3.:

$$q = (r_{s+1} - 2) + (r_{s+2} - 2) + \cdots + (r_n - 2),$$

andererseits

$$p = (r_{s+1} - 1) + (r_{s+2} - 1) + \cdots + (r_n - 1),$$

folglich:

$$p - q = n - s, \quad s = n - p + q.$$

Hierin ist der Riemann-Rochsche Satz enthalten, dem wir, mit Rücksicht auf § 27, für diesen Fall folgenden Ausdruck geben können: **Sind A, B Ergänzungsklassen erster Gattung, von denen wenigstens die eine eine eigentliche ist, und a, b ihre Ordnungen, also**

$$a + b = 2p - 2,$$

so ist

$$(O, A) - \tfrac{1}{2}a = (O, B) - \tfrac{1}{2}b.$$

5. Wir können, wenn wir den Fall $(A, W) = 0$ nicht ausschließen, den Riemann-Rochschen Satz für beide Fälle dahin zusammenfassen:

Ist A eine eigentliche Klasse von der Ordnung n, so ist ihre Dimension

$$(O, A) = n - p + 1 + (A, W).$$

Da die Dimension einer eigentlichen Klasse (wenn sie nicht aus dem einzigen Nulleck besteht) mindestens $= 2$ sein muß, so folgt noch, wenn $(A, W) = 0$ ist,

$$n \gtrless p + 1,$$

und daraus der von Riemann herrührende Satz:

Jede Funktion, deren Ordnung $\leqq p$ ist, ist eine Funktion erster Gattung.

6. Es läßt sich mit Hilfe dieser Sätze leicht beweisen, daß die Hauptklasse W der vollständigen Polygone erster Gattung stets eine eigentliche ist.

Ist nämlich $\mathfrak{M}$ der Teiler von W, so läßt sich nach § 19, 2. in W ein Polygon $\mathfrak{A}\mathfrak{M}$ derart finden, daß $\mathfrak{A}$ relativ prim zu $\mathfrak{M}$ ist Die Klasse A von $\mathfrak{A}$ ist eine eigentliche (§ 21, 3.), und zugleich ist $\mathfrak{A}\mathfrak{M}$ das einzige durch $\mathfrak{A}$ teilbare Polygon der Klasse W (weil jedes Polygon in W den Teiler $\mathfrak{M}$ hat). Also ist

$$(A, W) = 1.$$

Nun ist p die Dimension von W, also auch die von A, und mithin nach dem Riemann-Rochschen Satze die Ordnung von A gleich $2p-2$, d. h. ebenso groß wie die von W. Mithin ist $\mathfrak{M} = \mathfrak{O}$.

§ 29.

Der Riemann-Rochsche Satz für uneigentliche Klassen erster Gattung.

Ist A eine Klasse erster Gattung vom Teiler $\mathfrak{M}$ und

$$A = \mathfrak{M}A',$$

so ist A' eine eigentliche Klasse erster Gattung. Es sei B die Ergänzungsklasse von A; B' die von A'; a, b die Ordnungen der Klassen A, B; m die Ordnung von $\mathfrak{M}$. Die gesamte Klasse B erhält man, wenn man in sämtlichen durch $\mathfrak{M}$ teilbaren Polygonen der Klasse B' den Faktor $\mathfrak{M}$ unterdrückt; denn ist

$$\mathfrak{A}\mathfrak{B} = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W},$$

so gehört $\mathfrak{M}\mathfrak{B}$ in die Klasse B', und umgekehrt, wenn

$$\mathfrak{A}'\mathfrak{B}' = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W}$$

ist, so gehört $\mathfrak{B}$ in die Klasse B.

Hieraus ergibt sich aber nach § 21, 2.

$$(O, B) \geqq (O, B') - m.$$

Nun ist A' eine eigentliche Klasse von derselben Dimension wie A und von der Ordnung $a-m$, also (§ 28, 5.)

$$(O, A) = (O, A') = a - m - p + 1 + (A', W),$$

oder

$$(O, A) = (O, B') - m + a - p + 1;$$

daher

$$(O, A) \gtreqless (O, B) + a - p + 1 = (O, B) + \tfrac{1}{2}(a-b),$$

also

$$(O, A) - \tfrac{1}{2}a \gtreqless (O, B) - \tfrac{1}{2}b.$$

Da aber die Klassen A, B miteinander vertauscht werden können, so folgt in gleicher Weise

$$(O, B) - \tfrac{1}{2} b \gtrless (O, A) - \tfrac{1}{2} a,$$

d. h.

$$(O, A) - \tfrac{1}{2} a = (O, B) - \tfrac{1}{2} b,$$

wodurch der Riemann-Rochsche Satz in derselben Form wie in § 28, 4. für Polygonklassen erster Gattung allgemein nachgewiesen ist*).

§ 30.

Uneigentliche Klassen zweiter Gattung.

Es soll nun die Bedingung aufgesucht werden, unter der eine Polygonklasse zweiter Gattung A von der Ordnung n überhaupt eine uneigentliche sein kann, wobei sich die allgemeine Gültigkeit des Riemann-Rochschen Satzes von selbst ergeben wird.

1. Jede Klasse A kann stets durch Multiplikation mit einer andern Klasse N von der Ordnung ν in eine eigentliche Klasse AN verwandelt werden. Denn ist $\mathfrak{A}$ ein beliebiges Polygon in A, so wähle man eine Variable z, welche in sämtlichen Punkten von $\mathfrak{A}$ endlich bleibt (§ 15, 6.). Ist dann η eine beliebige Funktion des durch $\mathfrak{A}$ erzeugten Ideals in z, so ist das Obereck von η durch $\mathfrak{A}$ teilbar, also von der Form $\mathfrak{A}\mathfrak{N}$, und die Klasse von $\mathfrak{A}\mathfrak{N}$ ist eine eigentliche.

2. Die Dimension der eigentlichen Klasse AN zweiter Gattung ist nach § 28, 3.

$$(O, AN) = n + \nu - p + 1,$$

und hieraus folgt nach § 21, 2.

$$(O, A) \gtrless n - p + 1.$$

Ist nun der Teiler $\mathfrak{M}$ der Klasse A von der Ordnung m, und

$$A = \mathfrak{M} A',$$

---

*) Nach der Ausdrucksweise von Christoffel (Über die kanonische Form der Riemannschen Integrale erster Gattung, Annali di Matematica pura ed applicata, Serie II, Tomo IX) ist

$$(A, W) + a - p = (O, B) + a - p = (O, A) - 1$$

der „Überschuß“,

$$(A, W) - 1 = (O, B) - 1$$

der „Defekt“ des Punktsystems $\mathfrak{A}$.

so ist A' eine eigentliche Klasse von derselben Dimension wie A, und mithin (§ 28, 5.)

$$(O, A) = (O, A') = n - m - p + 1 + (A', W),$$

also

$$(A', W) \gtreqless m,$$

d. h. A' muß gewiß von der ersten Gattung sein, wenn A eine uneigentliche Klasse ist. Ist also B' die Ergänzungsklasse von A', so ist auch

$$(O, B') \gtreqless m.$$

Wäre aber $(O, B' > m$, so würde sich nach § 20, 2. in B' ein durch $\mathfrak{M}$ teilbares Polygon $\mathfrak{M}\mathfrak{B}$ finden lassen und es wäre

$$\mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

also A von der ersten Gattung, gegen die Voraussetzung. Es ist also

$$(A', W) = m$$

und folglich

$$(O, A) = n - p + 1,$$

worin wieder der Riemann-Rochsche Satz für diesen Fall, genau in der Form von § 28, 3. enthalten ist.

3. Enthält die Klasse A nur ein einziges isoliertes Polygon, so ist $(O, A) = n - p + 1 = 1$, mithin $n = p$, d. h. ein isoliertes Polygon zweiter Gattung hat stets die Ordnung p. Umgekehrt ist, nach 2. jedes Polygon zweiter Gattung von der Ordnung p ein isoliertes.

4. Unter Beibehaltung der Bezeichnung von 2. ist $(O, B') = m$ und daher läßt sich nach dem oft angewandten Satze (§ 20, 2.) in B' ein durch ein beliebiges $(m-1)$-Eck teilbares Polygon finden. Setzt man also, indem man einen beliebigen Punkt $\mathfrak{P}$ von $\mathfrak{M}$ absondert,

$$\mathfrak{M} = \mathfrak{P}\mathfrak{M}',$$

so ist ein Polygon $\mathfrak{M}'\mathfrak{B}$ in B' enthalten und also

$$\mathfrak{A}'\mathfrak{M}'\mathfrak{B} = \mathfrak{W}.$$

Das Polygon $\mathfrak{A}'\mathfrak{M}' = \mathfrak{A}''$ und seine Klasse A'' sind daher von der ersten Gattung, und A hat, wenn P die Klasse von $\mathfrak{P}$ bedeutet die Form

$$A = PA''.$$

Zugleich muß $(A'', W) = (O, B'') = 1$ sein, d. h. die Ergänzungsklasse B'' von A'' enthält nur ein einziges isoliertes Polygon $\mathfrak{B}''$, da sonst in B'' ein durch $\mathfrak{P}$ teilbares Polygon existieren würde, und also auch A gegen die Voraussetzung von der ersten Gattung wäre.

5. Ist umgekehrt A'' eine Klasse erster Gattung, für welche $(A'', W) = 1$, so daß die Ergänzungsklasse B'' von A'' aus einem isolierten Polygon $\mathfrak{B}''$ besteht; ist ferner $\mathfrak{P}$ ein in B'' nicht aufgehender Punkt, und seine Klasse P, so ist $A = PA''$ eine uneigentliche Klasse zweiter Gattung von der Ordnung n, in deren Teiler $\mathfrak{P}$ aufgeht.

Daß A von der zweiten Gattung ist, ergibt sich zunächst aus der Annahme, daß $\mathfrak{P}$ in $\mathfrak{B}''$ nicht aufgeht. Die Dimension von A ist daher nach 2.

$$(O, A) = n - p + 1,$$

wo n die Ordnung von A bedeutet; andererseits ist die Dimension der Klasse A'' nach §§ 28 und 29:

$$(O, A'') = n - p + (A'', W) = n - p + 1;$$

also sind A und A'' von derselben Dimension. Sämtliche Polygone der Klasse A'' gehen aber durch Multiplikation mit $\mathfrak{P}$ in Polygone der Klasse A über, und wegen der Gleichheit der Dimensionen wird hierdurch auch die letzte Klasse vollständig erschöpft. Es enthalten daher sämtliche Polygone der Klasse A den Faktor $\mathfrak{P}$, der sonach auch im Teiler von A aufgeht.

6. In dem besonderen Falle, wo das Geschlecht p des Körpers Ω den Wert 0 hat, kommen Polygone und Klassen erster Gattung überhaupt nicht vor. Es existieren also in diesem Falle auch keine uneigentlichen Klassen. Die Dimension einer jeden Klasse ist um 1 größer als ihre Ordnung. Insbesondere gehört also auch jeder Punkt $\mathfrak{P}$ zu einer eigentlichen Klasse von der Dimension 2, und daher existieren in diesem Falle in Ω Funktionen z, welche von der ersten Ordnung sind. Durch eine solche läßt sich jede andere Funktion des Körpers rational ausdrücken, denn die zwischen z und einer anderen Variablen des Körpers bestehende irreduktible Gleichung ist in bezug auf letztere vom ersten Grad (§ 15, 7.).

§ 31.

Die Differentiale zweiter und dritter Gattung.

1. Ist jetzt nach der in § 25 eingeführten Bezeichnung

$$d\tilde{\omega} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

ein beliebiges Differential in Ω, also, wenn a, b die Ordnungen von $\mathfrak{A}$ und $\mathfrak{B}$ sind,

$$a = b + 2p - 2,$$

und werden $\mathfrak{A}$, $\mathfrak{B}$ als relativ prim vorausgesetzt, so muß, wenn $\mathfrak{U}$, $\mathfrak{Z}$ Untereck und Verzweigungspolygon für eine beliebige Variable z bedeuten, $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$ äquivalent sein (§ 25). Bezeichnet man also mit U, Z, A, B die Klassen der Polygone $\mathfrak{U}$, $\mathfrak{Z}$, $\mathfrak{A}$, $\mathfrak{B}$, so muß

$$U^2 A = Z B$$

sein. Andererseits ist aber, wenn W die Hauptklasse erster Gattung ist,

$$U^2 W = Z,$$

woraus sich die Relation

$$A = BW$$

ergibt. Ist umgekehrt $\mathfrak{A}$ ein beliebiges Polygon der Klasse BW, so folgt daraus die Äquivalenz von $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$, also die Existenz eines Differentials von der Bezeichnung $\frac{\mathfrak{A}}{\mathfrak{B}}$. Daraus ergibt sich, daß $\mathfrak{B}$ dann und nur dann Untereck eines Differentials $d\tilde{\omega}$ sein kann, wenn in BW ein zu $\mathfrak{B}$ relativ primes Polygon existiert, d. h. wenn der Teiler der Klasse BW relativ prim zu $\mathfrak{B}$ ist. Die Dimension der Klasse BW gibt dann zugleich die Dimension der zum Untereck $\mathfrak{B}$ gehörigen Schar von Differentialen $d\tilde{\omega}$ (§ 25). Die Sätze § 30, 4., 5. ergeben daher, da $(W, W) = 1$ ist, das folgende Resultat.

a) Besteht $\mathfrak{B}$ aus einem einzigen Punkt (ist $b = 1$), so ist die Klasse BW eine uneigentliche mit dem Teiler $\mathfrak{B}$; also kann die Ordnung b des Unterecks eines Differentials $d\tilde{\omega}$ nicht gleich Eins sein.

b) Ist $b \geqq 2$, so ist BW stets eine eigentliche Klasse zweiter Gattung und daher ihre Dimension

$$b + p - 1.$$

Untereck eines Differentials kann also jedes beliebige Polygon von mehr als einem Punkt sein, und es existieren unter den zu einem Untereck von der Ordnung b gehörigen Differentialen $b + p - 1$ linear unabhängige.

2. Wir suchen jetzt unter der Voraussetzung, daß $b \gtreqless 2$ ist, für die Klasse A eine Basis derart auf, daß jedes Element $\mathfrak{A}_r$ dieser Basis ein Differential $d\tilde{\omega}_r$ von möglichst einfacher Beschaffenheit liefert, nämlich ein solches, dessen Untereck eine Potenz eines einzelnen Punktes oder das Produkt aus nur zwei verschiedenen Punkten ist.

Angenommen, es sei für die Klasse BW eine solche Basis bereits gefunden

(1) $$\mathfrak{A}_1,\ \mathfrak{A}_2,\ \mathfrak{A}_3,\ \ldots\ \mathfrak{A}_{b+p-1},$$

so bilden wir daraus, wenn P die Klasse eines beliebigen Punktes $\mathfrak{P}$ bedeutet, eine ebensolche Basis für die Klasse BPW von der Dimension $b+p$, nämlich

(2) $$\mathfrak{P}\mathfrak{A}_1,\ \mathfrak{P}\mathfrak{A}_2,\ \ldots\ \mathfrak{P}\mathfrak{A}_{b+p-1},\ \mathfrak{A}'.$$

Die ersten $b+p-1$ dieser Polygone gehören wirklich der Klasse BPW an und sind voneinander unabhängig, weil es die Polygone (1) sind; zugleich sind die aus ihnen gebildeten Differentiale

$$d\tilde{\omega}_r = \frac{\mathfrak{P}\mathfrak{A}_r}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{A}_r}{\mathfrak{B}}$$

mit den aus (1) gebildeten identisch. Es kommt also nur noch auf die Bildung von $\mathfrak{A}'$ an, wobei zwei Fälle zu unterscheiden sind.

a) Geht $\mathfrak{P}$ in $\mathfrak{B}$ auf und ist $\mathfrak{B} = \mathfrak{M}\mathfrak{P}^m$, $\mathfrak{M}$ nicht durch $\mathfrak{P}$ teilbar, so ist $P^{m+1}W$ eine eigentliche Klasse (weil $m+1 \geqq 2$, § 30, 4.), in welcher folglich ein durch $\mathfrak{P}$ nicht teilbares Polygon $\mathfrak{N}$ existiert; setzt man nun $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$, so gehört $\mathfrak{A}'$ der Klasse BPW an und ist durch $\mathfrak{P}$ nicht teilbar, folglich auch nicht in der Schar $(\mathfrak{P}\mathfrak{A}_1,\ \mathfrak{P}\mathfrak{A}_2,\ \ldots\ \mathfrak{P}\mathfrak{A}_{b+p-1})$, deren Teiler $\mathfrak{P}$ ist, enthalten; mithin sind die Polygone (2) unabhängig voneinander, und da ihre Anzahl $b+p$ ist, so bilden sie eine Basis der Klasse BPW. Das aus $\mathfrak{A}'$ gebildete Differential

$$d\tilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}^{m+1}}$$

hat die geforderte Form, da sein Untereck eine Potenz eines einzelnen Punktes ist.

b) Geht $\mathfrak{P}$ nicht in $\mathfrak{B}$ auf, so wähle man ein für allemal einen in $\mathfrak{B}$ aufgehenden Punkt $\mathfrak{P}_1$ und setze $\mathfrak{B} = \mathfrak{M}\mathfrak{P}_1$ (gleichgültig ob $\mathfrak{M}$ durch $\mathfrak{P}_1$ teilbar ist oder nicht). Man wähle sodann in der eigentlichen Klasse PP_1W ein durch $\mathfrak{P}$ und $\mathfrak{P}_1$ nicht teilbares Polygon $\mathfrak{N}$, so gehört $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$ wieder in die Klasse PBW, und da $\mathfrak{A}'$ nicht durch $\mathfrak{P}$ teilbar ist, so folgt wie oben, daß die Polygone (2) eine Basis von BPW bilden. Zugleich ist

$$d\tilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}\mathfrak{P}_1},$$

also von der verlangten Form.

Es bleibt noch übrig, den Anfang dieser Operation zu beschreiben. Ist $b = 0$, also $\mathfrak{B} = \mathfrak{O}$, so ist

$$BW = W = (\mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p)$$

(die Hauptklasse erster Gattung).

Ist $b = 2$, so wähle man aus der eigentlichen Klasse BW ein Polygon $\mathfrak{N}$, welches relativ prim zu $\mathfrak{B}$ ist; dann ist

$$BW = (\mathfrak{B}\mathfrak{W}_1, \mathfrak{B}\mathfrak{W}_2, \ldots \mathfrak{B}\mathfrak{W}_p, \mathfrak{N}).$$

Geht man von dieser Basis aus, um in der oben beschriebenen Weise eine Basis (1) zu bestimmen, die dem beliebig gegebenen Polygon

$$\mathfrak{B} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\mathfrak{P}_3^{m_3}\ldots$$

entspricht, und bestimmt die beiden Polygone $\mathfrak{A}_r'$, $\mathfrak{B}_r'$ aus der Bedingung

$$d\tilde{\omega}_r = \frac{\mathfrak{A}_r}{\mathfrak{B}} = \frac{\mathfrak{A}_r'}{\mathfrak{B}_r'},$$

so daß sie keinen gemeinschaftlichen Teiler haben, so sind die Polygone $\mathfrak{B}_r'$, die als Unterecke der Differentiale $d\tilde{\omega}_r$ auftreten, folgende:

a) p-mal tritt der Nenner $\mathfrak{O}$ auf, und die zugehörigen Differentiale $d\tilde{\omega}_r$ sind die Differentiale erster Gattung.

b) Je einmal treten die Unterecke $\mathfrak{P}_1^2$, $\mathfrak{P}_1^3$, ... $\mathfrak{P}_1^{m_1}$ (wenn $m_1 \geqq 2$), $\mathfrak{P}_2^2$, $\mathfrak{P}_2^3$, ... $\mathfrak{P}_2^{m_2}$; $\mathfrak{P}_3^2$, $\mathfrak{P}_3^3$, ... $\mathfrak{P}_3^{m_3}$, ... auf.

Die zu den Unterecken $\mathfrak{P}^r$ gehörigen Differentiale $d\omega_r$ werden, wenn eine genauere Unterscheidung nötig ist, mit $dt_{(\mathfrak{P}^{r-1})}$ bezeichnet und heißen Differentiale zweiter Gattung.

c) Endlich treten die Produkte $\mathfrak{P}_1\mathfrak{P}_2$, $\mathfrak{P}_1\mathfrak{P}_3$, ... (bei festgehaltenem $\mathfrak{P}_1$) je einmal auf. Die zugehörigen Differentiale $d\tilde{\omega}_r$ werden mit $d\pi_{(\mathfrak{P}_1, \mathfrak{P}_r)}$ bezeichnet und heißen Differentiale dritter Gattung.

Jedes Differential $d\tilde{\omega}$, dessen Untereck $\mathfrak{B}$ ist, kann in der Form dargestellt werden

$$d\tilde{\omega} = \sum^{r} c_r d\tilde{\omega}_r \tag{3}$$

mit konstanten Koeffizienten c_r, welche die Normalform des Differentials $d\tilde{\omega}$ genannt wird. Hat man jedes der einzelnen Differentiale $d\tilde{\omega}_r$ auf eine bestimmte Art gewählt, so läßt sich die Normalform auch nur auf eine einzige Weise herstellen, was unmittelbar aus der linearen Unabhängigkeit der Differentiale $d\tilde{\omega}_r$ folgt.

§ 32.

Die Residuen.

1. Ist $d\tilde{\omega}$ ein beliebiges Differential in $\mathfrak{Q}$ und $\mathfrak{P}$ ein Punkt, der m-mal im Untereck $\mathfrak{B}$ desselben vorkommt ($m \gtreqless 0$), so wähle man eine Variable z so, daß sie in $\mathfrak{P}$ ∞^1 wird. Es läßt sich dann (nach § 15, 4.), und zwar nur auf eine Weise, setzen

$$(1) \qquad \frac{d\tilde{\omega}}{dz} = a_{m-2}z^{m-2} + a_{m-3}z^{m-3} + \cdots + a_1 z + a_0 + a_{-1}z^{-1} + \eta z^{-2},$$

worin die a Konstanten, η eine Funktion in $\mathfrak{Q}$, die in $\mathfrak{P}$ endlich ist. Der Koeffizient $-a_{-1}$ von $-z^{-1}$ in diesem Ausdruck heißt das Residuum des Differentials $d\tilde{\omega}$ in bezug auf den Punkt $\mathfrak{P}$. Aus dieser Definition ergeben sich die folgenden Sätze:

2. Das Residuum in bezug auf einen Punkt $\mathfrak{P}$ kann nur dann von Null verschieden sein, wenn $m > 0$, d. h. wenn der Punkt $\mathfrak{P}$ im Untereck von $d\tilde{\omega}$ wirklich vorkommt, und ist daher für die Differentiale erster Gattung immer gleich 0.

3. Das Residuum einer Summe von Differentialen ist gleich der Summe der Residuen der einzelnen Differentiale.

4. Das Residuum eines eigentlichen Differentials ist stets gleich 0. Ist nämlich σ eine Funktion in $\mathfrak{Q}$, und wenn die b Konstanten, σ' eine in $\mathfrak{P}$ endliche Funktion bedeuten,

$$\sigma = b_m z^m + b_{m-1}z^{m-1} + \cdots + b_1 z + \sigma',$$

so ergibt sich durch Differentiation dieses Ausdruckes nach z, da $\frac{d\sigma'}{dz}$ in $\mathfrak{P}$ unendlich klein von mindestens zweiter Ordnung ist (§ 23, 10.), daß in dem Ausdruck für $\frac{d\sigma}{dz}$ ein Glied mit z^{-1} gar nicht vorkommt, womit die Behauptung erwiesen ist.

5. Das Residuum eines Differentials $d\tilde{\omega}$ ist unabhängig von der Wahl der Veränderlichen z. Ist nämlich z_1 eine zweite Veränderliche von derselben Beschaffenheit wie z, also, wenn a konstant, ζ in $\mathfrak{P}$ endlich ist:

$$(2) \qquad z = az_1 + \zeta,$$

so ergibt sich, wenn zur Abkürzung

$$\alpha = \frac{a_{m-2}z^{m-1}}{m-1} + \frac{a_{m-3}z^{m-2}}{m-2} + \cdots + a_0 z$$

gesetzt wird:

$$\frac{d\tilde{\omega}}{dz_1} = \frac{d\tilde{\omega}}{dz}\frac{dz}{dz_1} = \frac{d\alpha}{dz_1} + a_{-1}z^{-1}\frac{dz}{dz_1} - \eta\frac{dz^{-1}}{dz_1}.$$

Nun ist, wenn ζ', ζ'' in $\mathfrak{P}$ endliche Funktionen sind, wie sich nach § 23 und § 15, 4. leicht ergibt:

$$z^{-1}\frac{dz}{dz_1} = z_1^{-1} + z_1^{-2}\zeta', \qquad \frac{dz^{-1}}{dz_1} = z_1^{-2}\zeta'',$$

und daraus folgt nach 3., 4. die Richtigkeit der aufgestellten Behauptung*).

6. Die Summe der Residuen eines jeden Differentials $d\tilde{\omega}$ in bezug auf alle Punkte $\mathfrak{P}$ ist stets gleich Null.

Beim Beweise dieses wichtigen Satzes können wir uns auf die Betrachtung der Residuen beschränken, welche zu den sämtlichen im Untereck $\mathfrak{B}$ von $d\tilde{\omega}$ aufgehenden voneinander verschiedenen Punkten gehören; wir fügen jedoch zu diesen noch so viele voneinander verschiedene willkürliche Punkte mit verschwindenden Residuen hinzu, bis wir ein aus lauter einfachen Punkten bestehendes einer eigentlichen Klasse angehöriges Polygon $\mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_n$ erhalten. Dann wählen wir eine Variable z von der Ordnung n, deren Untereck eben dies Polygon ist, welche also in jedem der Punkte $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_n$ und nur in diesen ∞^1 wird. Unter diesen finden sich dann sämtliche voneinander verschiedene in $\mathfrak{B}$ aufgehende Punkte. Es ergibt sich unter dieser Voraussetzung für $\iota = 1, 2, \ldots n$

$$(3)\quad \frac{d\tilde{\omega}}{dz} = a^{(\iota)}_{m-2}z^{m-2} + a^{(\iota)}_{m-3}z^{m-3} + \cdots + a^{(\iota)}_0 + a^{(\iota)}_{-1}z^{-1} + \eta^{(\iota)}z^{-2},$$

wo $\eta^{(\iota)}$ eine in $\mathfrak{P}_\iota$ endliche Funktion bedeutet. Lassen wir für die Konstanten $a^{(\iota)}$ auch den Wert 0 zu, so kann der Exponent m unabhängig von ι angenommen werden (m ist dann, wenn nicht alle $a^{(\iota)}_{m-2}$ verschwinden, der Exponent der höchsten Potenz eines einzelnen Punktes, welche in $\mathfrak{B}$ vorkommt). Der zu beweisende Satz besteht dann darin, daß $\sum_\iota a^{(\iota)}_{-1} = 0$ ist. Um ihn zu beweisen, bilden wir die Spur der Funktion $\frac{d\tilde{\omega}}{dz}$ für die Variable z (§ 2) und bedienen

*) Man kann bei der Definition des Residuums auch eine Veränderliche r zugrunde legen, die in $\mathfrak{P}$ unendlich klein in der ersten Ordnung ist. Ist dann

$$\frac{d\tilde{\omega}}{dr} = a_m r^{-m} + \cdots + a_1 r^{-1} + \eta$$

und η in $\mathfrak{P}$ endlich, so ist a_1 das Residuum von $d\tilde{\omega}$ in bezug auf $\mathfrak{P}$.

uns dabei einer Erweiterung des Verfahrens § 16, 4. Wir wählen ein Funktionensystem $\varrho_1, \varrho_2, \dots \varrho_n$ in $\mathfrak{Q}$ folgendermaßen: Es sei

$\varrho_1 = 0^m$ in $\mathfrak{P}_2, \mathfrak{P}_3, \dots \mathfrak{P}_n$, endlich und von Null verschieden in $\mathfrak{P}_1$,
$\varrho_2 = 0^m$ in $\mathfrak{P}_1, \mathfrak{P}_3, \dots \mathfrak{P}_n$, „ „ „ „ „ „ $\mathfrak{P}_2$,
. . . . . .
$\varrho = 0^m$ in $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_{n-1}$, „ „ „ „ „ „ $\mathfrak{P}_n$.

Sind nun $x_1, x_2, \dots x_n$ rationale Funktionen von z, und ist

$$\eta = x_1\varrho_1 + x_2\varrho_2 + \cdots + x_n\varrho_n$$

eine Funktion in $\mathfrak{Q}$, welche für $z = \infty$, d. h. in $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_n$ endlich ist, so müssen $x_1, x_2, \dots x_n$ für $z = \infty$ endlich sein. Sind nämlich die $x_1, x_2, \dots x_n$ für $z = \infty$ nicht alle endlich, so existiert ein positiver Exponent r von der Beschaffenheit, daß die Produkte $x_1 z^{-r}, x_2 z^{-r}, \dots x_n z^{-r}$ für $z = \infty$ alle endlich sind, und mindestens eines von ihnen, etwa $x_1 z^{-r}$ von Null verschieden; dann enthält aber die Gleichung

$$\eta z^{-r} = x_1 z^{-r}\varrho_1 + \cdots + x_n z^{-r}\varrho_n$$

den Widerspruch, daß im Punkte $\mathfrak{P}_1$ die linke Seite und alle Glieder der rechten Seite mit Ausnahme des ersten verschwinden.

Hieraus ergibt sich zugleich, wenn man $\eta = 0$ setzt, daß die Funktionen $\varrho_1, \varrho_2, \dots \varrho_n$ eine Basis von $\mathfrak{Q}$ bilden. Setzt man daher, indem man mit $x_{\iota,\iota'}$ rationale Funktionen von z bezeichnet,

$$\frac{d\widetilde{\omega}}{dz}\varrho_\iota = x_{\iota,1}\varrho_1 + x_{\iota,2}\varrho_2 + \cdots + x_{\iota,n}\varrho_n, \qquad (\iota = 1, 2, \dots n) \tag{4}$$

so ist (§ 2)

$$S\left(\frac{d\widetilde{\omega}}{dz}\right) = x_{1,1} + x_{2,2} + \cdots + x_{n,n}. \tag{5}$$

Nun ist, wie aus (3) hervorgeht, $z^{-m+2}\dfrac{d\widetilde{\omega}}{dz}\varrho_\iota$ für $z = \infty$ endlich und daraus ergibt sich nach der soeben bewiesenen Eigenschaft der Funktionen ϱ, daß auch

$$z^{-m+2}x_{\iota,\iota'}$$

für $z = \infty$ endlich sind. Nun sind z. B. in dem Punkte $\mathfrak{P}_2$ die Funktionen $\varrho_1, \varrho_3, \dots \varrho_n$ unendlich klein in der m^{ten} Ordnung, während ϱ_2 dort endlich und von Null verschieden ist. Daher werden in $\mathfrak{P}_2$ die Funktionen

$$z\frac{d\widetilde{\omega}}{dz}\varrho_1, \quad zx_{1,1}\varrho_1, \quad zx_{1,3}\varrho_3, \dots zx_{1,n}\varrho_n$$

alle verschwinden, und es muß mithin auch $z\,x_{1,2}$ für $z = \infty$ verschwinden. Das gleiche folgt für $z\,x_{1,3}, \ldots z\,x_{1,n}$ und allgemein für $z\,x_{\iota,\iota'}$, sobald ι, ι' voneinander verschieden sind. Daher wird $z^2 x_{\iota,\iota'}$ für $z = \infty$ endlich sein.

Setzt man nun, indem man x_ι eine neue rationale Funktion bedeuten läßt,

$$(6) \qquad x_{\iota,\iota} = a^{(\iota)}_{m-2} z^{m-2} + a^{(\iota)}_{m-3} z^{m-3} + \cdots + a^{(\iota)}_{-1} z^{-1} + x_\iota z^{-2},$$

so folgt aus (3)

$$x_{\iota,\iota} - \frac{d\widetilde{\omega}}{dz} = z^{-2}(x_\iota - \eta^{(\iota)}),$$

und aus (4)

$$(\eta^{(\iota)} - x_\iota)\varrho_\iota = z^2 x_{\iota,1}\varrho_1 + \cdots + z^2 x_{\iota,\iota-1}\varrho_{\iota-1} + z^2 x_{\iota,\iota+1}\varrho_{\iota+1} + \cdots + z^2 x_{\iota,n}\varrho_n.$$

Da nun in $\mathfrak{P}_\iota$ $\eta^{(\iota)}$ endlich und ϱ_ι von Null verschieden, ferner alle Glieder der rechten Seite Null sind, so folgt, daß auch x_ι im Punkte $\mathfrak{P}_\iota$, und mithin, da es rational ist, für $z = \infty$ endlich ist. Aus (5) und (6) ergibt sich dann

$$(7)\; S\left(\frac{d\widetilde{\omega}}{dz}\right) = \sum^{\iota} a^{(\iota)}_{m-2} z^{m-2} + \sum^{\iota} a^{(\iota)}_{m-3} z^{m-3} + \cdots + \sum^{\iota} a^{(\iota)}_{-1} z^{-1} + \sum^{\iota} x_\iota z^{-2}.$$

Nun ist aber andererseits, wenn wieder $\mathfrak{U}$ das Untereck, $\mathfrak{Z}$ das Verzweigungspolygon von z ist:

$$\frac{d\widetilde{\omega}}{dz} = \frac{\mathfrak{U}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}},$$

und $\mathfrak{B}$ enthält keinen Punkt, der nicht auch in $\mathfrak{U}$ enthalten ist. Daraus ergibt sich wie in § 26, daß $\frac{d\widetilde{\omega}}{dz}$, als Funktion von z aufgefaßt, eine Funktion des zu $\mathfrak{o}$ komplementären Moduls $\mathfrak{e}$ ist, und mithin ist

$$S\left(\frac{d\widetilde{\omega}}{dz}\right)$$

eine ganze rationale Funktion von z (§ 11, 4.). Beachtet man dies, so folgt aus (7) $\sum^{\iota} x_\iota = 0$ und ferner der zu beweisende Satz

$$\sum^{(\iota)} a^{(\iota)}_{-1} = 0.$$

Wir können diesem Satze auch den folgenden Ausdruck geben: Das Residuum eines Differentials zweiter Gattung $dt_{(\mathfrak{P})}$ in bezug auf den Punkt $\mathfrak{P}$ ist Null.

Die Residuen eines Integrals dritter Gattung $d\pi_{(\mathfrak{P}_1,\mathfrak{P}_2)}$ in bezug auf $\mathfrak{P}_1$, $\mathfrak{P}_2$ sind einander gleich und entgegengesetzt, und sicher von

Null verschieden, da sonst $d\pi$ ein Differential erster Gattung sein würde.

Aus diesen Bemerkungen ergibt sich noch mittelst 4., daß ein eigentliches Differential $d\sigma$, in der Normalform dargestellt, kein Differential dritter Gattung enthalten kann. Es verdient ferner erwähnt zu werden, daß die Residuen des logarithmischen Differentials $\frac{d\sigma}{\sigma}$ ganze Zahlen, nämlich die Ordnungszahlen der Funktion σ sind (zufolge § 23).

§ 33.

Relationen zwischen Differentialen erster und zweiter Gattung.

1. Es sei σ eine Funktion in $\mathfrak{Q}$ mit dem Untereck

$$\mathfrak{B}' = \mathfrak{P}_1^{m_1-1}\mathfrak{P}_2^{m_2-1}\ldots \qquad (m_1, m_2, \ldots \geqq 2)$$

und dem Verzweigungspolygon (§ 16)

$$\mathfrak{S} = \mathfrak{S}'\mathfrak{P}_1^{m_1-2}\mathfrak{P}_2^{m_2-2}\ldots,$$

worin $\mathfrak{S}'$ durch die als verschieden vorausgesetzten Punkte $\mathfrak{P}_1, \mathfrak{P}_2 \cdots$ nicht teilbar ist. Demnach ist in der symbolischen Bezeichnung von § 25 das eigentliche Differential

$$d\sigma = \frac{\mathfrak{S}}{\mathfrak{B}'^2} = \frac{\mathfrak{S}'}{\mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots},$$

woraus zunächst hervorgeht, daß ein eigentliches Differential niemals von der ersten Gattung sein kann.

2. Das eigentliche Differential $d\sigma$, welches in seiner Darstellung durch die Normalform nur Differentiale erster und zweiter Gattung enthalten kann, gehört zu der Schar derjenigen Differentiale, deren Untereck

$$\mathfrak{B} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots = \mathfrak{B}'\mathfrak{P}_1\mathfrak{P}_2\ldots$$

ist. Umgekehrt wird man also auch in einer solchen Schar, vorausgesetzt daß $m_1, m_2, \ldots \geqq 2$ sind, und daß $\mathfrak{B}'$ zu einer eigentlichen Polygonklasse gehört, stets mindestens ein eigentliches Differential $d\sigma$ finden. Denn dazu ist nach 1. nur erforderlich, daß in $\mathfrak{Q}$ eine Funktion σ mit dem Untereck $\mathfrak{B}'$ existiert.

3. Hieraus ergibt sich nun der folgende wichtige Satz. **Alle Differentiale zweiter Gattung lassen sich linear mit konstanten Koeffizienten darstellen durch p besondere passend gewählte Differentiale zweiter Gattung, durch Differentiale erster Gattung und durch eigentliche Differentiale.**

Um dies einzusehen, wähle man ein beliebiges Polygon zweiter Gattung $\mathfrak{A}$ von der Ordnung p. Ist nun $\mathfrak{P}$ ein beliebiger Punkt, r ein positiver Exponent, so ist das Polygon $\mathfrak{A}\mathfrak{P}^r$ gleichfalls von der zweiten Gattung, und folglich kann der Teiler $\mathfrak{M}$ der zugehörigen Klasse nicht durch $\mathfrak{P}$ teilbar sein, weil sonst $\mathfrak{A}\mathfrak{P}^{r-1}$, also auch $\mathfrak{A}$ ein Polygon erster Gattung wäre (§ 30, 4.). Setzt man daher

$$\mathfrak{A}\mathfrak{P}^r = \mathfrak{M}\mathfrak{B}',$$

so wird $\mathfrak{P}$ nicht in $\mathfrak{M}$ aufgehen, und folglich enthält $\mathfrak{B}'$ den Faktor $\mathfrak{P}$ genau r-mal öfter als $\mathfrak{A}$. Zugleich gehört $\mathfrak{B}'$ in eine eigentliche Klasse. Ist nun

$$\mathfrak{B}' = \mathfrak{P}^m\mathfrak{P}'^{m'}\mathfrak{P}''^{m''}\ldots,$$

so gehen die Punktpotenzen $\mathfrak{P}^m$, $\mathfrak{P}'^{m'}$, $\mathfrak{P}''^{m''}$, ... alle in $\mathfrak{A}$ auf. Setzen wir also

$$\mathfrak{B} = \mathfrak{P}^{m+r+1}\mathfrak{P}'^{m'+1}\mathfrak{P}''^{m''+1}\ldots = \mathfrak{B}'\mathfrak{P}\mathfrak{P}'\mathfrak{P}''\ldots,$$

so existiert nach 2. in der zu dem Untereck $\mathfrak{B}$ gehörigen Differentialschar gewiß ein eigentliches Differential $d\sigma$. Die Darstellung desselben durch die Normalform enthält sicher das Differential

$$(1) \qquad dt_{(\mathfrak{P}^{m+r})}$$

und außerdem alle oder einige der Differentiale

$$(2) \qquad \begin{cases} dt_{(\mathfrak{P})},\ dt_{(\mathfrak{P}^2)},\ \ldots\ dt_{(\mathfrak{P}^m)}\ldots dt_{(\mathfrak{P}^{m+r-1})}, \\ dt_{(\mathfrak{P}')},\ dt_{(\mathfrak{P}'^2)},\ \ldots\ dt_{(\mathfrak{P}'^{m'})}, \\ dt_{(\mathfrak{P}'')},\ dt_{(\mathfrak{P}''^2)},\ \ldots\ dt_{(\mathfrak{P}''^{m''})} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

nebst Differentialen erster Gattung. Es läßt sich also das Differential (1) linear und mit konstanten Koeffizienten durch (2), durch Differentiale erster Gattung und durch $d\sigma$ ausdrücken.

Ist daher das p-Eck zweiter Gattung

$$\mathfrak{A} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots,$$

so erkennt man durch wiederholte Anwendung des hier beschriebenen Verfahrens, daß alle Differentiale zweiter Gattung in der Weise, wie unser Satz es ausspricht, darstellbar sind durch die p Differentiale

$$(3) \qquad \begin{cases} dt_{(\mathfrak{P}_1)}\ldots dt_{(\mathfrak{P}_1^{m_1})}, \\ dt_{(\mathfrak{P}_2)}\ldots dt_{(\mathfrak{P}_2^{m_2})}, \\ \ldots\ldots\ldots \end{cases}$$

Braunschweig und Königsberg i. Pr., im Oktober 1880.

Erläuterungen zur vorstehenden Abhandlung.

In der vorstehenden Abhandlung, mit der die arithmetische Theorie der algebraischen Funktionen geschaffen wurde, zerfällt der Aufbau der Theorie in drei Stufen. Der erste, formale Teil bezieht sich auf den Bereich der ganzen und gebrochenen algebraischen Funktionen einer Unbestimmten; im zweiten Teil bildet die arithmetisch definierte, absolute Riemannsche Fläche die Grundlage. Der dritte Teil — der nur am Schluß des Vorworts erwähnt, aber nicht erschienen ist — sollte von der arithmetischen zur topologischen absoluten Riemannschen Fläche übergehen: ein Begriff, der auf anderer Grundlage erst mehr als dreißig Jahre später in der Weylschen „Idee der Riemannschen Fläche" entwickelt wurde. Es verdient daher besonders hervorgehoben zu werden, daß (§ 16) scharf darauf hingewiesen ist, daß die absolute Riemannsche Fläche ein zu dem Körper gehöriger invarianter Begriff ist, von dem aus sich der Übergang zur Riemannschen Auffassung vollziehen läßt.

Der erste Teil läßt sich dadurch charakterisieren, daß der algebraische Funktionenkörper als hyperkomplexes System über dem Grundkörper der rationalen Funktionen einer Unbestimmten betrachtet wird. Tatsächlich sind die Methoden zur Definition von Norm, Spur, Diskriminante usw. diejenigen der Darstellungstheorie hyperkomplexer Systeme; die Betrachtungen aus § 6 und § 22 etwa sind solche über reduzible Darstellungen.

Die um die absolute Riemannsche Fläche sich gruppierenden Entwicklungen des zweiten Teils — insbesondere die Begriffe des „Punktes" und des „Divisors" (Polygons) — sind allgemeiner bekannt geworden durch das Buch von Hensel-Landsberg, wo aber die idealtheoretischen Grundlagen des ersten Teils durch funktionentheoretische ersetzt sind. Hensel-Landsberg führen die Gruppe aller ganzen und gebrochenen Divisoren ein, was Vereinfachungen beim Beweis des Riemann-Rochschen Satzes nach sich zieht. Der einfachste Beweis ergibt sich aber erst, wenn man die bei Dedekind-Weber, § 22, gegebene Konstruktion der Normalbasis auf gebrochene Ideale überträgt, und dann nach Hensel-Landsberg weiter schließt.

Die wesentlichsten Entwicklungen von Hensel-Landsberg wurden von Jung (Rend. Palermo 26, und spätere Arbeiten) auf algebraische Funktionenkörper von zwei Veränderlichen übertragen. Eine rein arithmetische Begründung der Divisoren, die erst nach Weiterentwicklung der Idealtheorie möglich war, wurde von Schmeidler (Math. Zeitschr. 28) und v. d. Waerden (Math. Ann. 101) für n Veränderliche gegeben. Es handelt sich dort immer um Divisoren der Höchstdimension; arithmetische Definition und Existenzbeweis für den allgemeinen invarianten Punktbegriff bei algebraischen Mannigfaltigkeiten findet sich bei v. d. Waerden (Math. Ann. 97).

Noether.

XIX.

Über die Diskriminanten endlicher Körper.

[Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Bd. 29, S. 1—56 (1882).]

Unter den charakteristischen Zahlen oder Invarianten, von denen die Eigenschaften eines endlichen Zahlkörpers Ω abhängen, ist nächst dem Grade vor allem die Grundzahl oder Diskriminante $\Delta(\Omega)$ zu nennen*), und es ist von großer Wichtigkeit für die Zahlentheorie und Algebra, die Bildung dieser ganzen rationalen Zahl auf allgemeine Gesetze zurückzuführen. In den Göttingischen gelehrten Anzeigen vom 20. September 1871 (S. 1490) habe ich zuerst einen hierauf bezüglichen Satz ohne Beweis mitgeteilt, durch welchen die in der Grundzahl aufgehenden Primzahlen bestimmt werden; so einfach und naheliegend dieser Satz ist, so war es mir doch erst nach vielen vergeblichen Anstrengungen im Juli 1871 gelungen, ihn streng und allgemein zu beweisen; es treten nämlich hierbei dieselben eigentümlichen Umstände als hemmende Schwierigkeiten auf, die ich schon damals erwähnt habe, und die später in der Abhandlung**) Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen eingehend dargestellt sind. In der gegenwärtigen Abhandlung, welche als eine Fortsetzung der eben genannten anzusehen ist, werden zunächst zwei verschiedene Beweise für den oben erwähnten Satz gegeben, in § 3 ein unvollständiger, in den §§ 4—6 ein vollständiger, welcher im wesentlichen mit dem im Juli 1871 gefundenen übereinstimmt. Der übrige, und zwar größere Teil der Abhandlung ist aber einer genaueren Untersuchung der Grundzahl gewidmet und führt zu einem allgemeinen Gesetze, von welchem die Konstitution dieser Zahl beherrscht wird; das Resultat, zu welchem man gelangt, besteht darin, daß die Grund-

*) Hinsichtlich der von mir benutzten Kunstausdrücke muß ich auf meine anderen Schriften verweisen, namentlich auf das Supplement XI in der dritten Auflage der Vorlesungen über Zahlentheorie von Dirichlet, die ich im folgenden mit Z. zitieren werde.

**) Bd. 23 dieser Abhandlungen, 1878. Dieselbe soll mit G. zitiert werden.

zahl, absolut genommen, immer die Norm eines Ideals ist, welches ich das Grundideal des Körpers Ω nenne, und dessen Zusammensetzung aus Primidealen, abgesehen von gewissen singulären Fällen, vollständig bestimmt wird; und hieraus folgt ohne weiteres ein dritter Beweis des oben erwähnten Satzes.

Dieser Satz gestattet, was ich schon am Schlusse der früheren Abhandlung ausgesprochen habe, noch eine wesentliche Erweiterung, und ich füge hinzu, daß dasselbe auch von allen übrigen in der vorliegenden Abhandlung gewonnenen Resultaten gilt. Zu dieser wichtigen Verallgemeinerung gelangt man, wenn man den Körper der rationalen Zahlen, soweit er als solcher in unserer Untersuchung auftritt, überall durch einen beliebigen in Ω als Divisor enthaltenen Körper ersetzt; die Modifikationen, welche unsere Resultate hierdurch erleiden, bestehen im wesentlichen nur darin, daß neben den gewöhnlichen Normen, Diskriminanten, Spuren auch partielle oder relative, auf diesen Körper bezügliche Normen usw. einzuführen, und gewisse rationale Zahlen durch Ideale dieses Körpers zu ersetzen sind. Da aber diese Erweiterung mancherlei Vorbereitungen und einen beträchtlichen Raum erfordert, so muß ihre Darstellung einer besonderen Abhandlung vorbehalten bleiben.

§ 1.

Ist Ω ein endlicher Körper n^{ten} Grades (Z. §§ 162—164), so geht derselbe durch n Permutationen $\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(n)}$ in n konjugierte Körper $\Omega^{(1)}, \Omega^{(2)} \dots \Omega^{(n)}$ über, und wir wollen, wenn θ irgend eine Zahl in Ω bedeutet, mit $\theta^{(1)}, \theta^{(2)} \dots \theta^{(n)}$ die konjugierten Zahlen bezeichnen, welche durch diese Permutationen aus θ erzeugt werden. Führt man eine Variable t ein, so entspricht jeder Zahl θ eine zugehörige ganze Funktion

$$(1) \qquad \begin{aligned} F(t) &= (t-\theta^{(1)})(t-\theta^{(2)})\dots(t-\theta^{(n)}) \\ &= t^n + a_1 t^{n-1} + a_2 t^{n-2} + \dots + a_{n-1} t + a_n, \end{aligned}$$

deren Koeffizienten rationale Zahlen $1, a_1, a_2 \dots a_n$ sind. Diese Funktion erhält man auch auf folgende Weise. Bilden die n Zahlen $\omega_1, \omega_2 \dots \omega_n$ eine beliebige Basis des Körpers Ω, so kann man

$$(2) \qquad \begin{aligned} \theta\omega_1 &= e_{1,1}\omega_1 + e_{2,1}\omega_2 + \dots + e_{n,1}\omega_n \\ \theta\omega_2 &= e_{1,2}\omega_1 + e_{2,2}\omega_2 + \dots + e_{n,2}\omega_n \\ &\dots\dots\dots\dots\dots\dots\dots \\ \theta\omega_n &= e_{1,n}\omega_1 + e_{2,n}\omega_2 + \dots + e_{n,n}\omega_n \end{aligned}$$

setzen, wo die Koeffizienten $e_{r,s}$ rationale Zahlen bedeuten, und es ist

$$(3)\qquad (-1)^n F(t) = \begin{vmatrix} e_{1,1}-t, & e_{2,1} & \dots e_{n,1} \\ e_{1,2}, & e_{2,2}-t & \dots e_{n,2} \\ \dots & \dots & \dots \\ e_{1,n}, & e_{2,n} & \dots e_{n,n}-t \end{vmatrix}.$$

Die mit $N(\theta)$ zu bezeichnende Norm der Zahl θ ist das Produkt aus allen mit θ konjugierten Zahlen, also

$$(4)\qquad N(\theta) = \theta^{(1)}\theta^{(2)}\dots\theta^{(n)} = (-1)^n a_n = \begin{vmatrix} e_{1,1}\dots e_{n,1} \\ \dots \\ e_{1,n}\dots e_{n,n} \end{vmatrix}.$$

Die der Zahl θ entsprechende Funktion $F(t)$ kann daher auch dadurch definiert werden, daß für jeden rationalen Wert von t

$$(5)\qquad F(t) = N(t-\theta)$$

ist.

Da die Funktion $F(t)$, also auch ihre Derivierte $F'(t)$ durch die Zahl θ vollständig bestimmt ist, so gilt dasselbe von der Zahl $F'(\theta)$, welche wir zur Abkürzung mit θ^* bezeichnen wollen, weil sie häufig auftreten wird; bedeutet $\varphi^{(1)}$ die identische Permutation des Körpers Ω (d. h. diejenige, durch welche jede Zahl θ in sich selbst übergeht), so ist hiernach

$$(6)\qquad \begin{aligned} \theta^* = F'(\theta) &= (\theta-\theta^{(2)})(\theta-\theta^{(3)})\dots(\theta-\theta^{(n)}) \\ &= n\,\theta^{n-1} + (n-1)\,a_1\,\theta^{n-2} + \dots + a_{n-1}; \end{aligned}$$

bekanntlich ist die Funktion $F(t)$ stets und nur dann irreduktibel, wenn diese Zahl θ^* nicht verschwindet.

Die Diskriminante $\Delta(\alpha_1, \alpha_2 \dots \alpha_n)$ eines beliebigen Systems von n Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$, welche dem Körper Ω angehören, ist das Quadrat der aus den konjugierten Zahlen $\alpha_r^{(s)}$ gebildeten Determinante, also

$$(7)\qquad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \begin{vmatrix} \alpha_1^{(1)}, & \alpha_2^{(1)} \dots \alpha_n^{(1)} \\ \alpha_1^{(2)}, & \alpha_2^{(2)} \dots \alpha_n^{(2)} \\ \dots & \dots \\ \alpha_1^{(n)}, & \alpha_2^{(n)} \dots \alpha_n^{(n)} \end{vmatrix}^2;$$

sie ist stets und nur dann von Null verschieden, wenn $\alpha_1, \alpha_2 \dots \alpha_n$ eine Basis des Körpers Ω bilden. Ist

$$(8)\qquad \begin{cases} \alpha_1 = a_{1,1}\omega_1 + a_{2,1}\omega_2 + \dots + a_{n,1}\omega_n \\ \alpha_2 = a_{1,2}\omega_1 + a_{2,2}\omega_2 + \dots + a_{n,2}\omega_n \\ \dots \\ \alpha_n = a_{1,n}\omega_1 + a_{2,n}\omega_2 + \dots + a_{n,n}\omega_n, \end{cases}$$

wo die Koeffizienten $a_{r,s}$ rationale Zahlen bedeuten, so ist

$$(9)\quad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \left(\sum \pm a_{1,1} a_{2,2} \dots a_{n,n}\right)^2 \Delta(\omega_1, \omega_2 \dots \omega_n).$$

Die oben definierten Zahlen θ^* stehen in naher Beziehung zum Begriff der Diskriminante, denn es ist bekanntlich

$$(10)\quad \Delta(1, \theta, \theta^2 \dots \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(\theta^*).$$

Unter der Spur der Zahl θ verstehen wir die Summe aller mit ihr konjugierten Zahlen; wir bezeichnen diese offenbar rationale Zahl mit $S(\theta)$; dann ist

$$(11)\quad \begin{aligned} S(\theta) &= \theta^{(1)} + \theta^{(2)} + \dots + \theta^{(n)} = -a_1 \\ &= e_{1,1} + e_{2,2} + \dots + e_{n,n}, \end{aligned}$$

wo a_1 und die Größen $e_{r,s}$ dieselbe Bedeutung haben, wie in (1) und (2). Über den Gebrauch dieses Zeichens ist folgendes zu merken. Da jede rationale Zahl durch alle Permutationen in sich selbst übergeht, so ist

$$(12)\quad S(0) = 0, \quad S(1) = n;$$

da ferner $(\alpha \pm \beta)^{(r)} = \alpha^{(r)} \pm \beta^{(r)}$, und $(\alpha\beta)^{(r)} = \alpha^{(r)}\beta^{(r)}$ ist, so folgt

$$(13)\quad S(\alpha \pm \beta) = S(\alpha) \pm S(\beta),$$

und wenn c rational ist,

$$(14)\quad S(c\alpha) = c\,S(\alpha).$$

Ferner folgt aus

$$S(\alpha\beta) = \alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \dots + \alpha^{(n)}\beta^{(n)}$$

nach dem Satze über die Multiplikation der Determinanten

$$(15)\quad \sum \pm \alpha_1^{(1)} \alpha_2^{(2)} \dots \alpha_n^{(n)} \cdot \sum \pm \beta_1^{(1)} \beta_2^{(2)} \dots \beta_n^{(n)} = \begin{vmatrix} S(\alpha_1\beta_1) & \dots & S(\alpha_1\beta_n) \\ \dots & \dots & \dots \\ S(\alpha_n\beta_1) & \dots & S(\alpha_n\beta_n) \end{vmatrix},$$

mithin

$$(16)\quad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \begin{vmatrix} S(\alpha_1\alpha_1), & S(\alpha_1\alpha_2) \dots S(\alpha_1\alpha_n) \\ S(\alpha_2\alpha_1), & S(\alpha_2\alpha_2) \dots S(\alpha_2\alpha_n) \\ \dots & \dots \\ S(\alpha_n\alpha_1), & S(\alpha_n\alpha_2) \dots S(\alpha_n\alpha_n) \end{vmatrix}.$$

Hat eine Zahl α die Eigenschaft, daß für jede in $\mathfrak{Q}$ enthaltene Zahl ω die Spur $S(\alpha\omega)$ verschwindet, so ist gewiß $\alpha = 0$, weil

sonst für $\omega = \alpha^{-1}$ sich ein Widerspruch mit (12) ergeben würde; und hieraus folgt mit Rücksicht auf (13) allgemeiner, daß, wenn für jede Zahl ω die Gleichung

(17) $$S(\alpha\omega) = S(\beta\omega)$$

gilt, notwendig

(18) $$\alpha = \beta$$

ist.

§ 2.

Der Inbegriff $\mathfrak{o}$ aller in Ω enthaltenen ganzen Zahlen (Z. § 166) ist ein endlicher Modul

(1) $$\mathfrak{o} = [\omega_1, \omega_2 \dots \omega_n],$$

d. h. es gibt n ganze Zahlen $\omega_1, \omega_2 \dots \omega_n$ von der Beschaffenheit, daß jede ganze Zahl ω in der Form

(2) $$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

darstellbar ist, wo die Koeffizienten h_1, $h_2 \cdots h_n$ ganze rationale Zahlen bedeuten. Dieses System heißt eine Basis von $\mathfrak{o}$, und seine Diskriminante

(3) $$D = \Delta(\omega_1, \omega_2 \cdots \omega_n),$$

welche eine von Null verschiedene ganze rationale Zahl ist, heißt die Grundzahl oder Diskriminante des Körpers Ω.

Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ ganze Zahlen, so sind die in den Gleichungen (8) und (9) des vorigen Paragraphen auftretenden rationalen Koeffizienten $a_{r,s}$ ganze Zahlen; folglich ist die Diskriminante $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ teilbar durch D (und nur dann $= D$, wenn diese Zahlen ebenfalls eine Basis von $\mathfrak{o}$ bilden). Ist θ eine ganze Zahl, so kann man dies auf das System $1, \theta, \theta^2 \dots \theta^{n-1}$ anwenden und erhält

(4) $$\Delta(1, \theta, \theta^2 \dots \theta^{n-1}) = Dk^2 = \pm N(\theta^*),$$

wo k eine ganze rationale Zahl ist, die wir, wie früher (G. § 1), den Index der Zahl θ nennen wollen.

Ist ω eine beliebige ganze Zahl, so gilt dasselbe von den mit ihr konjugierten Zahlen, mithin ist die Spur $S(\omega)$ eine ganze rationale Zahl; und wenn ω durch die ganze rationale Zahl c teilbar ist, so ist $S(\omega)$ ebenfalls durch c teilbar, weil $\omega = c\alpha$, also $S(\omega) = cS(\alpha)$, und $S(\alpha)$ ganz ist.

Mit p bezeichnen wir im folgenden immer eine (positive) rationale Primzahl; dann folgt aus einer bekannten Eigenschaft der zum Exponenten p gehörenden Binomial-Koeffizienten, daß, wenn μ, ν irgend zwei ganze algebraische Zahlen bedeuten, immer

$$(\mu + \nu)^p = \mu^p + \nu^p + p\varrho \tag{5}$$

ist, wo ϱ ebenfalls eine ganze Zahl ist. Hieraus folgt, wenn ω irgend eine Zahl in $\mathfrak{o}$ bedeutet, zunächst

$$S(\omega)^p = (\omega^{(1)} + \omega^{(2)} + \cdots + \omega^{(n)})^p \equiv S(\omega^p) \pmod{p};$$

da aber $S(\omega)$ eine ganze rationale Zahl, mithin nach dem Satze von Fermat

$$S(\omega)^p \equiv S(\omega) \pmod{p}$$

ist, so ergibt sich

$$S(\omega) \equiv S(\omega^p) \pmod{p}, \tag{6}$$

und allgemeiner, wenn man ω immer durch ω^p ersetzt,

$$S(\omega) \equiv S(\omega^{p^m}) \pmod{p}. \tag{7}$$

Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen in $\mathfrak{o}$, so folgt hieraus mit Rücksicht auf die Gleichung (16) des vorigen Paragraphen der Satz

$$\Delta(\alpha_1^p, \alpha_2^p \cdots \alpha_n^p) \equiv \Delta(\alpha_1, \alpha_2 \cdots \alpha_n) \pmod{p}. \tag{8}$$

Ebenso ergibt sich aus (7) unmittelbar der folgende (nicht umzukehrende) Satz: Wenn ω durch alle in p aufgehenden Primideale teilbar ist, so ist

$$S(\omega) \equiv 0 \pmod{p}; \tag{9}$$

denn wenn man den Exponenten m hinreichend groß wählt, so wird die Zahl ω^{p^m} durch p teilbar.

§ 3.

Wir wenden uns nun zum Beweise des in der Einleitung erwähnten Satzes:

Die rationale Primzahl p geht stets und nur dann in der Grundzahl D des Körpers Ω auf, wenn p in diesem Körper durch das Quadrat eines Primideals teilbar ist.

Am Schlusse der früheren Abhandlung (G. § 5) ist bemerkt, daß dieser Beweis, falls es in $\mathfrak{o}$ eine Zahl θ gibt, deren Index k nicht teilbar durch p ist, leicht aus den dort gewonnenen Resultaten abgeleitet werden kann. Dies soll zunächst geschehen.

In der Tat, wenn es eine solche Zahl θ gibt, so ist damals gezeigt (G. § 2), daß die Zerlegung des Ideals $\mathfrak{o}p$ in Primfaktoren auf die Zerlegung der zugehörigen Funktion $F(t)$ in Primfunktionen nach dem Modul p zurückkommt. Ist nämlich

$$F(t) \equiv P(t)^e P_1(t)^{e_1} \cdots \pmod{p},$$

wo $P(t)$, $P_1(t)\cdots$ wesentlich verschiedene Primfunktionen bedeuten, so entsprechen denselben ebenso viele verschiedene Primideale $\mathfrak{p}, \mathfrak{p}_1 \cdots$, und gleichzeitig gilt die Zerlegung

$$\mathfrak{o}p = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots;$$

ist ferner $\psi(t)$ eine beliebige ganze Funktion von t mit ganzen rationalen Koeffizienten, so ist die ganze Zahl $\psi(\theta)$ stets und nur dann durch das Primideal $\mathfrak{p}$ teilbar, wenn $\psi(t)$ nach dem Modul p durch die entsprechende Primfunktion $P(t)$ teilbar ist. Verbinden wir hiermit den allgemeinen Satz*), daß eine Funktion $F(t)$ und ihre Derivierte $F'(t)$ stets und nur dann durch eine und dieselbe Primfunktion $P(t)$ nach p teilbar sind, wenn $F(t)$ durch das Quadrat von $P(t)$ teilbar ist, so ergibt sich folgendes.

Wenn p durch das Quadrat eines Primideals teilbar ist, so muß einer der Exponenten $e, e_1 \cdots$, z. B. $e > 1$ sein; dann ist $F'(t)$ durch $P(t)$, folglich die Zahl θ^* durch $\mathfrak{p}$ teilbar; mithin geht die Norm von $\mathfrak{p}$, welche immer durch p teilbar, nämlich eine Potenz von p ist, in der Norm von θ^* auf (Z. § 169, 5.); hieraus folgt mit Rücksicht auf die Gleichung (4) in § 2, daß Dk^2 durch p teilbar ist, und da p nicht in k aufgeht, so muß die Grundzahl D durch p teilbar sein.

Wenn aber p durch kein Primideal-Quadrat teilbar ist, so sind die Exponenten $e, e_1 \cdots$ sämtlich $= 1$; dann ist $F'(t)$ durch keine der Primfunktionen $P(t), P_1(t) \cdots$ teilbar, und folglich ist die Zahl θ^* auch durch keines der Primideale $\mathfrak{p}, \mathfrak{p}_1 \cdots$ teilbar; mithin ist θ^* relative

---

*) In meiner Abhandlung über die Theorie der höheren Kongruenzen (Borchardts Journal, Bd. 54, S. 7), die ich im folgenden wieder mit K. zitieren werde, ist zwar nur der erste Teil bewiesen, daß $F'(t)$ gewiß durch $P(t)$ teilbar ist, wenn $P(t)^2$ in $F(t)$ aufgeht; bedenkt man aber, daß die Derivierte $P'(t)$ niemals $\equiv 0 \pmod{p}$ ist (weil sonst die Primfunktion $P(t)$ der p^{ten} Potenz einer Funktion kongruent wäre), und daß folglich $P'(t)$ auch nicht durch $P(t)$ teilbar sein kann (weil der Grad von $P'(t)$ kleiner als der von $P(t)$ ist), so ergibt sich auch der andere Teil des obigen Satzes.

Primzahl zu p, und hieraus folgt (Z. § 174, 8), daß ihre Norm $\pm D k^2$, und also auch deren Teiler D nicht durch p teilbar ist.

Hiermit ist der obige Satz vollständig bewiesen, aber nur unter der Voraussetzung der Existenz einer Zahl θ, deren Index k nicht durch p teilbar ist; da nun in der früheren Abhandlung (G. § 5) gezeigt ist, daß es Körper Ω gibt, bei denen diese Voraussetzung nicht für alle Primzahlen p zutrifft, so bedarf es eines anderen Beweises, um die Wahrheit des Satzes für alle Fälle außer Zweifel zu setzen.

§ 4.

Der zu beweisende Satz zerfällt in zwei Teile, von denen der eine in folgender Form ausgesprochen werden kann:

Ist p durch das Quadrat eines Primideals teilbar, so geht p in der Grundzahl D auf.

Dies ist sehr leicht zu beweisen. Denn wenn $\mathfrak{o}\,p = \mathfrak{a}\,\mathfrak{p}^2$ ist, wo $\mathfrak{p}$ ein Primideal (oder auch irgend ein von $\mathfrak{o}$ verschiedenes Ideal) bedeutet, so ist $\mathfrak{a}\,\mathfrak{p}$ nicht teilbar durch $\mathfrak{o}\,p$, und es gibt folglich in $\mathfrak{a}\,\mathfrak{p}$ eine durch p nicht teilbare Zahl ω; da ferner $(\mathfrak{a}\,\mathfrak{p})^2 = \mathfrak{a}\,p$, also durch $\mathfrak{o}\,p$ teilbar ist, so geht p in ω^2, also auch in ω^p auf. Setzt man nun wieder

$$\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n],$$

also

$$D = \Delta(\omega_1, \omega_2 \cdots \omega_n),$$

so ist

$$\omega = \sum h_i \omega_i,$$

wo die ganzen rationalen Koordinaten $h_1, h_2 \cdots h_n$ nicht alle durch p teilbar sind, weil sonst auch ω durch p teilbar wäre, was nicht der Fall ist. Erhebt man zur p^{ten} Potenz, so folgt aus dem Satze (5) in § 2 mit Rücksicht auf den Satz von Fermat

$$\omega^p \equiv \sum (h_i \omega_i)^p \equiv \sum h_i \omega_i^p \pmod{p},$$

und da ω^p durch p teilbar ist, so ist auch

$$\sum h_i \omega_i^p \equiv 0 \pmod{p}.$$

Da aber die Zahlen h_i, wie oben bemerkt, nicht alle durch p teilbar sind, so folgt aus einem früher bewiesenen Satze (Z. § 166, (1)), daß die Diskriminante

$$\Delta(\omega_1^p, \omega_2^p \cdots \omega_n^p)$$

durch p (sogar durch p^2) teilbar ist*), und hieraus ergibt sich nach dem Satze (8) in § 2, daß p auch in D aufgeht, w. z. b. w.

§ 5.

Bei weitem schwieriger ist der zweite Teil des Satzes, die Umkehrung des ersten Teils, zu beweisen, und wir müssen zunächst einige Hilfssätze entwickeln, die aber auch für verwandte Untersuchungen von Nutzen sind.

1. Satz: Ist die aus lauter ganzen rationalen Zahlen $c_{r,s}$ gebildete Determinante n^{ten} Grades

$$C = \begin{vmatrix} c_{1,1}, & c_{2,1} \cdots c_{n,1} \\ c_{1,2}, & c_{2,2} \cdots c_{n,2} \\ \cdots & \cdots \\ c_{1,n}, & c_{2,n} \cdots c_{n,n} \end{vmatrix}$$

teilbar durch die Primzahl p, so kann man n ganze rationale Zahlen $x_1, x_2 \cdots x_n$, die nicht alle durch p teilbar sind, so wählen, daß die n Kongruenzen

$$\left.\begin{aligned} c_{1,1}x_1 + c_{1,2}x_2 + \cdots + c_{1,n}x_n &\equiv 0 \\ c_{2,1}x_1 + c_{2,2}x_2 + \cdots + c_{2,n}x_n &\equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ c_{n,1}x_1 + c_{n,2}x_2 + \cdots + c_{n,n}x_n &\equiv 0 \end{aligned}\right\} \text{(mod. } p\text{)}$$

erfüllt werden**).

Dies leuchtet von selbst ein, wenn alle Koeffizienten $c_{r,s}$ durch p teilbar sind. Im entgegengesetzten Falle wird es eine Unterdeterminante C' von höchstem Grade $m < n$ geben, welche nicht durch p teilbar ist, und wir dürfen annehmen, es sei

$$C' = \begin{vmatrix} c_{1,1}, & c_{1,2} \cdots c_{1,m} \\ c_{2,1}, & c_{2,2} \cdots c_{2,m} \\ \cdots & \cdots \\ c_{m,1}, & c_{m,2} \cdots c_{m,m} \end{vmatrix};$$

dann genügt man allen vorstehenden Kongruenzen z. B. dadurch,

*) Dies gilt offenbar auch dann, wenn die Potenzen $\omega_1^p, \omega_2^p \cdots \omega_n^p$ keine Basis des Körpers Ω bilden, weil in diesem Falle ihre Diskriminante verschwindet, also durch p teilbar ist.

**) Von demselben Satze ist auch schon in der früheren Abhandlung (G. § 1) Gebrauch gemacht; der Vollständigkeit wegen soll jetzt der Beweis nachgeholt werden.

daß man

$$x_{m+2} = 0, \quad x_{m+3} = 0 \cdots x_n = 0$$

und für $x_1, x_2 \cdots x_m, x_{m+1}$ resp. die Koeffizienten setzt, mit welchen die unbestimmten Größen $u_1, u_2 \cdots u_m, u_{m+1}$ in der Determinante

$$\begin{vmatrix} c_{1,1}, & c_{1,2} \cdots c_{1,m}, & c_{1,m+1} \\ c_{2,1}, & c_{2,2} \cdots c_{2,m}, & c_{2,m+1} \\ \cdots & \cdots & \cdots \\ c_{m,1}, & c_{m,2} \cdots c_{m,m}, & c_{m,m+1} \\ u_1, & u_2 \cdots u_m, & u_{m+1} \end{vmatrix}$$

multipliziert sind; denn diese Determinante

$$u_1 x_1 + u_2 x_2 + \cdots + u_m x_m + u_{m+1} x_{m+1}$$

wird zufolge unserer Annahme immer eine durch p teilbare Zahl, sobald

$$u_1 = c_{r,1}, \quad u_2 = c_{r,2} \cdots u_m = c_{r,m}, \quad u_{m+1} = c_{r,m+1}$$

gesetzt wird. Und da $x_{m+1} = C'$, also nicht durch p teilbar ist, so ist der Satz bewiesen*).

2. Sind $\alpha_1, \alpha_2 \cdots \alpha_r$ bestimmte Zahlen in $\mathfrak{o}$, während $x_1, x_2 \cdots x_r$ willkürliche ganze rationale Zahlen bedeuten, so bilden die Zahlen

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_r \alpha_r$$

einen durch $\mathfrak{o}$ teilbaren endlichen Modul $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_r]$, und die Anzahl $(\mathfrak{a}, \mathfrak{o}\, p)$ der in $\mathfrak{a}$ enthaltenen, nach p inkongruenten Zahlen ist offenbar höchstens $= p^r$; sie wird stets und nur dann genau $= p^r$ sein, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ die Eigenschaft haben, daß die Kongruenz $\alpha \equiv 0 \pmod{p}$ nur durch $x_1 \equiv 0, x_2 \equiv 0 \cdots x_r \equiv 0 \pmod{p}$ befriedigt werden kann; in diesem Fall wollen wir sagen, daß die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ ein nach p irreduktibeles System bilden, und es leuchtet ein, daß $r \leqq n$ ist, weil $(\mathfrak{o}, \mathfrak{o}\, p) = p^n$ ist. Bilden die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ aber ein nach p reduktibeles System, gibt es also ganze rationale Zahlen $a_1, a_2 \cdots a_r$, welche die Kongruenz

$$a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_r \alpha_r \equiv 0 \pmod{p}$$

befriedigen, und von denen wenigstens eine, z. B. a_r, nicht durch p teilbar ist, so kann man, weil p eine Primzahl ist, eine ganze rationale Zahl a' so bestimmen, daß $a' a_r \equiv 1 \pmod{p}$ wird; multipliziert

*) Ersetzt man die oben benutzten Elemente $c_{r,m+1}$ sukzessive durch $c_{r,m+2}$, $c_{r,m+3} \cdots c_{r,n}$, so erhält man im ganzen $n - m$ partikuläre Lösungen der gegebenen Kongruenzen, aus welchen ihre allgemeinste Lösung leicht abzuleiten ist.

man die obige Kongruenz mit α', so folgt, daß

$$\alpha_r \equiv b_1 \alpha_1 + b_2 \alpha_2 + \cdots + b_{r-1} \alpha_{r-1} \pmod{p}$$

ist, wo $b_1, b_2 \cdots b_{r-1}$ ganze rationale Zahlen bedeuten, und hieraus ergibt sich, daß jede Zahl α des Moduls $\mathfrak{a}$ mit einer Zahl α' des Moduls $\mathfrak{a}' = [\alpha_1, \alpha_2 \cdots \alpha_{r-1}]$ nach p kongruent ist; da ferner $\mathfrak{a}'$ teilbar durch $\mathfrak{a}$, d. h. da jede Zahl α' auch in $\mathfrak{a}$ enthalten ist, so folgt $(\mathfrak{a}, \mathfrak{o}\, p) = (\mathfrak{a}', \mathfrak{o}\, p)$, und diese Anzahl ist höchstens $= p^{r-1}$. Ist das System $\alpha_1, \alpha_2 \cdots \alpha_{r-1}$ ebenfalls reduktibel nach p, so kann man in derselben Weise fortfahren, bis man zu einem nach p irreduktibelen System gelangt; besteht dasselbe aus m Zahlen, so ist

$$(\mathfrak{a}, \mathfrak{o}\, p) = p^m;$$

die Zahl m ist dadurch charakterisiert, daß es m Zahlen $\alpha'_1, \alpha'_2 \cdots \alpha'_m$ in $\mathfrak{a}$ gibt, welche ein nach p irreduktibeles System bilden, während jedes aus $(m+1)$ Zahlen des Moduls $\mathfrak{a}$ gebildete System reduktibel nach p ist; ist α eine beliebige Zahl in $\mathfrak{a}$, so gibt es immer m ganze rationale Zahlen $y_1, y_2 \cdots y_m$, welche die Kongruenz

$$\alpha \equiv y_1 \alpha'_1 + y_2 \alpha'_2 + \cdots + y_m \alpha'_m \pmod{p}$$

befriedigen und in bezug auf den Modul p vollständig bestimmt sind. (Wenn $\mathfrak{a}$ durch $\mathfrak{o}\, p$ teilbar ist, so ist $m = 0$ zu setzen.)

3. Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine Basis von $\mathfrak{o}$, und betrachtet man ein System von n ganzen Zahlen

$$\begin{aligned}
\alpha_1 &= c_{1,1}\omega_1 + c_{2,1}\omega_2 + \cdots + c_{n,1}\omega_n \\
\alpha_2 &= c_{1,2}\omega_1 + c_{2,2}\omega_2 + \cdots + c_{n,2}\omega_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n &= c_{1,n}\omega_1 + c_{2,n}\omega_2 + \cdots + c_{n,n}\omega_n,
\end{aligned}$$

so geht aus dem obigen Satze 1. hervor, daß dasselbe stets und nur dann nach p irreduktibel ist, wenn die aus den Koordinaten $c_{r,s}$ gebildete Determinante C nicht durch p teilbar ist. Unter dieser Voraussetzung gibt es daher, wenn ω eine gegebene ganze Zahl ist, immer n ganze rationale, nach dem Modul p vollständig bestimmte Zahlen $x_1, x_2 \cdots x_n$, welche die Kongruenz

$$\omega \equiv x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n \pmod{p}$$

befriedigen. Man kann daher auch

$$\left.\begin{aligned}
\omega\alpha_1 &\equiv x_{1,1}\alpha_1 + x_{2,1}\alpha_2 + \cdots + x_{n,1}\alpha_n \\
\omega\alpha_2 &\equiv x_{1,2}\alpha_1 + x_{2,2}\alpha_2 + \cdots + x_{n,2}\alpha_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\omega\alpha_n &\equiv x_{1,n}\alpha_1 + x_{2,n}\alpha_2 + \cdots + x_{n,n}\alpha_n
\end{aligned}\right\} \pmod{p}$$

setzen, wo die ganzen rationalen Zahlen $x_{r,s}$ nach dem Modul p bestimmt sind, und wir wollen den Satz*) beweisen, daß

$$S(\omega) \equiv x_{1,1} + x_{2,2} + \cdots + x_{n,n} \pmod{p}$$

ist.

In der Tat, da jede der Zahlen $\omega_1, \omega_2 \cdots \omega_n$ und folglich jede ganze Zahl durch Multiplikation mit C in eine Zahl des Moduls $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verwandelt wird, so kann man

$$\begin{aligned} C\omega\alpha_1 &= y_{1,1}\alpha_1 + y_{2,1}\alpha_2 + \cdots + y_{n,1}\alpha_n \\ C\omega\alpha_2 &= y_{1,2}\alpha_1 + y_{2,2}\alpha_2 + \cdots + y_{n,2}\alpha_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ C\omega\alpha_n &= y_{1,n}\alpha_1 + y_{2,n}\alpha_2 + \cdots + y_{n,n}\alpha_n \end{aligned}$$

setzen, wo die Koeffizienten $y_{r,s}$ ganze rationale Zahlen bedeuten, welche offenbar mit den obigen Koeffizienten $x_{r,s}$ durch die Kongruenzen

$$y_{r,s} \equiv C x_{r,s} \pmod{p}$$

zusammenhängen; da andererseits (zufolge § 1, (11) und (14))

$$S(C\omega) = C\,S(\omega) = y_{1,1} + y_{2,2} + \cdots + y_{n,n},$$

und C nicht durch p teilbar ist, so ergibt sich die Richtigkeit der zu beweisenden Kongruenz.

4. Wir zerlegen nun das Ideal $\mathfrak{o}p$ auf irgend eine Weise in ein Produkt von zwei Idealen $\mathfrak{p}$, $\mathfrak{q}$, und bezeichnen deren Grade**) resp. mit r, s; dann ist

$$\mathfrak{o}p = \mathfrak{p}\mathfrak{q};\quad N(\mathfrak{o}p) = p^n = N(\mathfrak{p})N(\mathfrak{q}) = p^r p^s,$$

also $r + s = n$. Da ferner (Z. § 173, 7)

$$(\mathfrak{q}, \mathfrak{o}p) = N(\mathfrak{p}) = p^r$$

ist, so gibt es (zufolge 2) in dem endlichen Modul $\mathfrak{q}$ ein System von r Zahlen

$$\varrho_0, \varrho_1 \cdots \varrho_{r-1},$$

welches irreduktibel nach p ist, und jede durch $\mathfrak{q}$ teilbare (d. h. in $\mathfrak{q}$ enthaltene) Zahl ist

$$\equiv h_0\varrho_0 + h_1\varrho_1 + \cdots + h_{r-1}\varrho_{r-1} \pmod{p},$$

*) Offenbar gelten ähnliche Sätze für $N(\omega)$ und alle übrigen Koeffizienten der zu ω zugehörigen Funktion n^{ten} Grades (§ 1).

**) Unter dem Grade eines beliebigen Ideals $\mathfrak{a}$ wird die Anzahl der (gleichen oder ungleichen) rationalen Primzahlen verstanden, deren Produkt $= N(\mathfrak{a})$ ist (vgl. Z. § 171, 10).

wo h_0, $h_1 \cdots h_{r-1}$ ganze rationale Zahlen bedeuten. Ebenso gibt es in $\mathfrak{p}$ ein nach p irreduktibeles System von s Zahlen

$$\sigma_0, \sigma_1 \cdots \sigma_{s-1},$$

und jede durch $\mathfrak{p}$ teilbare Zahl ist

$$\equiv k_0 \sigma_0 + k_1 \sigma_1 + \cdots + k_{s-1} \sigma_{s-1} \pmod{p},$$

wo k_0, $k_1 \cdots k_{s-1}$ ebenfalls ganze rationale Zahlen bedeuten.

Wir nehmen nun ferner an, daß $\mathfrak{p}$, $\mathfrak{q}$ relative Primideale sind, daß also $\mathfrak{o}$ ihr größter gemeinschaftlicher Teiler ist; dann läßt sich leicht zeigen, daß die n Zahlen

$$\varrho_0, \varrho_1 \cdots \varrho_{r-1}, \sigma_0, \sigma_1 \cdots \sigma_{s-1}$$

ebenfalls ein nach p irreduktibeles System bilden; da nämlich jede in $\mathfrak{o}$ enthaltene Zahl ω eine Summe von zwei Zahlen ist, deren eine in $\mathfrak{q}$, und deren andere in $\mathfrak{p}$ enthalten ist (Z. § 165 oder § 171), so ist auch

$$\omega \equiv h_0 \varrho_0 + \cdots + h_{r-1} \varrho_{r-1} + k_0 \sigma_0 + \cdots + k_{s-1} \sigma_{s-1} \pmod{p},$$

und hieraus ergibt sich unsere Behauptung (zufolge 2.), weil $(\mathfrak{o}, \mathfrak{o}\,p) = p^n = p^{r+s}$ ist. Dasselbe geht aber unmittelbar auch daraus hervor, daß die rechte Seite ω' der vorstehenden Kongruenz nur dann durch p teilbar wird, wenn alle n Koeffizienten h, $k \equiv 0 \pmod{p}$ sind; ist nämlich ω' durch p teilbar, so ist auch $\omega' \equiv 0 \pmod{\mathfrak{p}}$, mithin

$$h_0 \varrho_0 + \cdots + h_{r-1} \varrho_{r-1} \equiv 0 \pmod{\mathfrak{p}},$$

weil die Zahlen σ_0, $\sigma_1 \cdots \sigma_{s-1}$ in $\mathfrak{p}$ enthalten sind; da nun die linke Seite dieser Kongruenz auch in $\mathfrak{q}$ enthalten ist, so ist sie, weil $\mathfrak{p}$, $\mathfrak{q}$ relative Primideale sind, auch durch $\mathfrak{p}\,\mathfrak{q}$, also durch p teilbar, und folglich müssen die r Koeffizienten h durch p teilbar sein, weil $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ ein nach p irreduktibeles System bilden; und auf dieselbe Weise ergibt sich, daß auch die s Koeffizienten k durch p teilbar sein müssen, was zu zeigen war.

Nachdem dieser Punkt festgestellt ist, wollen wir den in 3. bewiesenen Satz über die Spur $S(\omega)$ auf unser System $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$, $\sigma_0, \sigma_1 \cdots \sigma_{s-1}$ und auf den Fall anwenden, daß ω eine beliebige durch $\mathfrak{q}$ teilbare Zahl μ ist. Da $\mathfrak{q}$ ein Ideal ist, so sind auch die r Produkte $\mu\varrho_0$, $\mu\varrho_1 \cdots \mu\varrho_{r-1}$ durch $\mathfrak{q}$ teilbar, und folglich wird

$$\left.\begin{aligned}
\mu\varrho_0 &\equiv h_{0,0}\,\varrho_0 + h_{1,0}\,\varrho_1 + \cdots + h_{r-1,0}\,\varrho_{r-1} \\
\mu\varrho_1 &\equiv h_{0,1}\,\varrho_0 + h_{1,1}\,\varrho_1 + \cdots + h_{r-1,1}\,\varrho_{r-1} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\mu\varrho_{r-1} &\equiv h_{0,r-1}\,\varrho_0 + h_{1,r-1}\,\varrho_1 + \cdots + h_{r-1,r-1}\,\varrho_{r-1}
\end{aligned}\right\} \pmod{p}.$$

Da ferner die übrigen s Produkte $\mu\sigma_0$, $\mu\sigma_1 \cdots \mu\sigma_{s-1}$ durch $\mathfrak{q}\mathfrak{p}$, also durch p teilbar sind, so werden in ihrer Darstellung durch die Zahlen ϱ, σ alle Koeffizienten $h, k \equiv 0 \pmod{p}$, und hieraus folgt nach dem in 3. bewiesenen Satze

$$S(\mu) \equiv h_{0,0} + h_{1,1} + \cdots + h_{r-1,r-1} \pmod{p}.$$

5. Wir nehmen jetzt, indem wir die bisherigen Voraussetzungen und Bezeichnungen beibehalten, ferner an, daß $\mathfrak{p}$ ein Primideal ist; unsere frühere Annahme, daß $\mathfrak{p}$ und $\mathfrak{q}$ relative Primideale sind, kommt also darauf hinaus, daß p nicht durch $\mathfrak{p}^2$ teilbar ist. Dann gilt der Satz, daß die Determinante

$$R = \begin{vmatrix} S(\varrho_0\varrho_0), & S(\varrho_0\varrho_1)\cdots & S(\varrho_0\varrho_{r-1}) \\ S(\varrho_1\varrho_0), & S(\varrho_1\varrho_1)\cdots & S(\varrho_1\varrho_{r-1}) \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ S(\varrho_{r-1}\varrho_0), & S(\varrho_{r-1}\varrho_1)\cdots & S(\varrho_{r-1}\varrho_{r-1}) \end{vmatrix}$$

nicht durch p teilbar ist. Wir bemerken zunächst, daß dieser Satz, wenn er für ein bestimmtes System $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ bewiesen ist, auch für jedes andere System $\varrho'_0, \varrho'_1 \cdots \varrho'_{r-1}$ gelten muß, welches dem Ideal $\mathfrak{q}$ angehört und nach p irreduktibel ist; man kann nämlich

$$\left.\begin{array}{l} \varrho'_0 \equiv a_{0,0}\varrho_0 + \cdots + a_{r-1,0}\varrho_{r-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \varrho'_{r-1} \equiv a_{0,r-1}\varrho_0 + \cdots + a_{r-1,r-1}\varrho_{r-1} \end{array}\right\} \pmod{p}$$

setzen, wo die aus den Koeffizienten $a_{\iota,\iota'}$ gebildete Determinante A nicht durch p teilbar ist, weil sonst (zufolge 1.) das System linker Hand reduktibel nach p wäre; da ferner, wenn die Summationsbuchstaben ι, ι' die Werte $0, 1 \cdots r-1$ durchlaufen,

$$\varrho'_h\varrho'_k \equiv \sum a_{\iota,h}a_{\iota',k}\varrho_\iota\varrho_{\iota'} \pmod{p},$$

also auch

$$S(\varrho'_h\varrho'_k) \equiv \sum a_{\iota,h}a_{\iota',k}S(\varrho_\iota\varrho_{\iota'}) \pmod{p}$$

ist, so ergibt sich aus bekannten Determinanten-Sätzen, daß die aus den Spuren $S(\varrho'_h\varrho'_k)$ gebildete Determinante $P'_\iota \equiv RA^2 \pmod{p}$ ist, woraus unsere obige Behauptung folgt.

Wir konstruieren nun ein bestimmtes nach p irreduktibeles System $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ auf folgende Weise. Da $\mathfrak{p}$ ein in p aufgehendes Primideal r^{ten} Grades ist, so wählen wir, wie in der früheren Abhandlung (G. § 4), eine ganze Funktion

$$(1) \qquad P(t) = t^r + a_1t^{r-1} + \cdots + a_{r-1}t + a_r$$

vom Grade r, welche ganze rationale Koeffizienten 1, $a_1 \cdots a_{r-1}$, a_r hat und eine Primfunktion in bezug auf den Modul p ist; dann hat die Kongruenz

(2) $$P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$$

immer r inkongruente Wurzeln, und wir bezeichnen mit α eine bestimmte von ihnen (die übrigen sind dann α^p, $\alpha^{p^2} \cdots \alpha^{p^{r-1}}$); sind ferner x_0, $x_1 \cdots x_{r-1}$ ganze rationale Zahlen, so kann, wie damals bewiesen ist, die Kongruenz

(3) $$x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{r-1}\alpha^{r-1} \equiv 0 \pmod{\mathfrak{p}}$$

nur dann bestehen, wenn diese Zahlen sämtlich durch p teilbar sind. Da ferner $\mathfrak{p}, \mathfrak{q}$ relative Primideale sind, so kann man immer eine Zahl ϱ so wählen, daß

(4) $$\varrho \equiv 1 \pmod{\mathfrak{p}}, \qquad \varrho \equiv 0 \pmod{\mathfrak{q}},$$

mithin

(5) $$\varrho^2 \equiv \varrho \pmod{p}$$

wird. Setzen wir nun

(6) $$\varrho_0 = \varrho,\ \varrho_1 = \varrho\alpha,\ \varrho_2 = \varrho\alpha^2 \cdots \varrho_{r-1} = \varrho\alpha^{r-1},$$

so sind diese r Zahlen in dem Ideal $\mathfrak{q}$ enthalten, weil ϱ in $\mathfrak{q}$ enthalten ist, und da die Kongruenz

$$x_0\varrho_0 + x_1\varrho_1 + \cdots + x_{r-1}\varrho_{r-1} \equiv 0 \pmod{p}$$

die obige Kongruenz (3) nach sich zieht, so bilden die Zahlen ϱ_0, $\varrho_1 \cdots \varrho_{r-1}$ ein nach p irreduktibles System in $\mathfrak{q}$.

Um für dieses System die Spuren $S(\varrho_i\varrho_{i'})$ und die zugehörige Determinante R zu bilden, dividieren wir alle Potenzen 1, t, $t^2 \cdots$ mit beliebig hohen Exponenten durch $P(t)$, wodurch Gleichungen von der Form

(7) $$t^m = c_0^{(m)} + c_1^{(m)}t + \cdots + c_{r-1}^{(m)}t^{r-1} + P(t)Q_m(t)$$

entstehen, in denen die Koeffizienten $c_i^{(m)}$ ganze rationale Zahlen bedeuten; da $Q_m(t)$ ebenfalls eine ganze Funktion mit ganzen rationalen Koeffizienten ist, so folgt

(8) $$\alpha^m \equiv c_0^{(m)} + c_1^{(m)}\alpha + \cdots + c_{r-1}^{(m)}\alpha^{r-1} \pmod{\mathfrak{p}}$$

und hieraus durch Multiplikation mit ϱ

(9) $$\varrho\alpha^m \equiv c_0^{(m)}\varrho_0 + c_1^{(m)}\varrho_1 + \cdots + c_{r-1}^{(m)}\varrho_{r-1} \pmod{p}.$$

Ersetzt man hierin m durch $m+1$, $m+2 \cdots m+r-1$ und bedenkt, daß $\varrho\alpha^m$ eine in $\mathfrak{q}$ enthaltene Zahl μ, und daß $\mu\varrho_i = \varrho^2\alpha^{m+i} \equiv \varrho\alpha^{m+i} \pmod{p}$ ist, so folgt aus dem in 4. bewiesenen Satze

(10) $$S(\varrho\alpha^m) \equiv s_m \pmod{p},$$

wo zur Abkürzung

$$s_m = c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{r-1}^{(m+r-1)} \tag{11}$$

gesetzt ist. Da ferner $\varrho_\iota \varrho_{\iota'} = \varrho^2 \alpha^{\iota+\iota'} \equiv \varrho\, \alpha^{\iota+\iota'}$ (mod. p), und folglich auch

$$S(\varrho_\iota \varrho_{\iota'}) \equiv S(\varrho\, \alpha^{\iota+\iota'}) \equiv s_{\iota+\iota'} \text{ (mod. } p) \tag{12}$$

ist, so ergibt sich die entsprechende Determinante

$$R \equiv \begin{vmatrix} s_0, & s_1 \cdots s_{r-1} \\ s_1, & s_2 \cdots s_r \\ s_{r-1}, & s_r \cdots s_{2r-2} \end{vmatrix} \text{ (mod. } p). \tag{13}$$

Um nun zu beweisen, daß diese aus den Zahlen s_m gebildete Determinante E nicht durch p teilbar ist, wollen wir folgenden Weg einschlagen. Bezeichnen wir mit ξ eine Wurzel der irreduktibelen Gleichung r^{ten} Grades

$$P(\xi) = 0, \tag{2'}$$

so ist ξ eine ganze Zahl, und der Inbegriff X aller durch ξ rational darstellbaren Zahlen ist ein Körper r^{ten} Grades, in welchem wir die Normen, Spuren und Diskriminanten resp. durch N', S' und Δ' bezeichnen wollen. Aus den Gleichungen (7) folgt nun zunächst

$$\xi^m = c_0^{(m)} + c_1^{(m)} \xi + \cdots + c_{r-1}^{(m)} \xi^{r-1}, \tag{7'}$$

und da die Zahlen $1, \xi, \xi^2 \cdots \xi^{r-1}$ eine Basis von X bilden, so ist (zufolge § 1, (11))

$$S'(\xi^m) = c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{r-1}^{(m+r-1)} = s_m, \tag{10'}$$

mithin (zufolge § 1, (16)) die Determinante

$$E = \Delta'(1, \xi, \xi^2 \cdots \xi^{r-1})$$

oder (zufolge § 1, (10))

$$E = (-1)^{\frac{r(r-1)}{2}} N'[P'(\xi)]. \tag{14}$$

Da nun $P'(t)$ und $P(t)$ relative Primfunktionen nach dem Modul p sind (§ 3, Anmerkung), so gibt es bekanntlich (K. § 4) zwei Funktionen $\varphi(t)$, $\psi(t)$, welche der Kongruenz

$$\varphi(t) P'(t) + \psi(t) P(t) \equiv 1 \text{ (mod. } p)$$

genügen, aus welcher

$$\varphi(\xi) P'(\xi) \equiv 1 \text{ (mod. } p)$$

folgt; mithin ist $P'(\xi)$ relative Primzahl zu p; dasselbe gilt folglich (Z. § 174, 2. und 8.) von ihrer Norm, also (zufolge (14)) auch von E und (zufolge (13)) von R, w. z. b. w.

Daß die aus den Zahlen s_m gebildete Determinante E nicht durch p teilbar ist, kann man auch ohne Einführung des Körpers X auf folgendem Wege beweisen. Zunächst sind aus den Definitionen (1), (7), (11) die bekannten Formeln abzuleiten:

$$s_{m+r} + a_1 s_{m+r-1} + \cdots + a_r s_m = 0 \tag{15}$$

und, wenn $k < r$,

$$s_k + a_1 s_{k-1} + \cdots + a_k s_0 = (r-k)\, a_k. \tag{16}$$

Drückt man nach (7) die einzelnen Glieder des durch $P(t)$ teilbaren Aggregates

$$P(t)\, t^m = t^{m+r} + a_1 t^{m+r-1} + \cdots + a_r t^m$$

durch die niedrigsten Potenzen von t aus, so ergibt sich

$$c_h^{(m+r)} + a_1 c_h^{(m+r-1)} + \cdots + a_r c_h^{(m)} = 0, \tag{17}$$

wo h jede beliebige der Zahlen $0, 1, 2 \cdots (r-1)$ ist; ersetzt man hierin m durch $(m+h)$ und summiert die so entstandenen Gleichungen für alle Werte von h, so erhält man unter Berücksichtigung von (11) die Gleichung (15). Ist ferner $m < r$, so folgt aus (7), daß

$$c_h^{(m)} = 1 \text{ oder } = 0 \tag{18}$$

ist, je nachdem m und h gleich oder verschieden sind*); ist nun k eine bestimmte der Zahlen $0, 1, 2 \cdots (r-1)$, so folgt aus (18) und (17), daß die Summe

$$c_h^{(k+h)} + a_1 c_h^{(k+h-1)} + \cdots + a_k c_h^{(h)} = a_k \text{ oder } = 0$$

ist, je nachdem

$$h \leqq r-1-k \quad \text{oder} \quad h \geqq r-k$$

ist; durch Summation aller dieser Gleichungen für die verschiedenen Werte von h ergibt sich (16). Hierauf setzen wir

$$P(t) - P(\alpha) = (t-\alpha)(\beta_0 + \beta_1 t + \beta_2 t^2 + \cdots + \beta_{r-1} t^{r-1}),$$

so ist

$$\text{(19)} \quad \begin{cases} \beta_0 &= \alpha^{r-1} + a_1 \alpha^{r-2} + \cdots + a_{r-2}\alpha + a_{r-1} \\ \beta_1 &= \alpha^{r-2} + a_1 \alpha^{r-3} + \cdots + a_{r-2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \beta_{r-2} &= \alpha + a_1 \\ \beta_{r-1} &= 1 \end{cases}$$

---

*) Hieraus und aus (17) folgt, daß das allgemeine Integral der Differenzengleichung r^{ter} Ordnung

$$y_{m+r} + a_1 y_{m+r-1} + \cdots + a_r y_m = 0$$

durch

$$y_m = c_0^{(m)} y_0 + c_1^{(m)} y_1 + \cdots + c_{r-1}^{(m)} y_{r-1}$$

ausgedrückt wird.

und

$$(20)\quad \begin{cases} \alpha\beta_0 &= P(\alpha) - a_r \equiv -a_r\beta_{r-1} \pmod{\mathfrak{p}} \\ \alpha\beta_1 &= \beta_0 - a_{r-1}\beta_{r-1} \\ \cdots\cdots\cdots\cdots\cdots \\ \alpha\beta_{r-2} &= \beta_{r-3} - a_2\beta_{r-1} \\ \alpha\beta_{r-1} &= \beta_{r-2} - a_1\beta_{r-1}. \end{cases}$$

Setzen wir ferner

$$(21)\qquad \eta_m = s_m\beta_0 + s_{m+1}\beta_1 + \cdots + s_{m+r-1}\beta_{r-1},$$

so folgt aus (15) und (20)

$$\alpha\eta_m \equiv \eta_{m+1} \pmod{\mathfrak{p}},$$

also

$$\eta_m \equiv \eta_0\alpha^m \pmod{\mathfrak{p}},$$

mithin

$$\eta_0\alpha^m \equiv s_m\beta_0 + s_{m+1}\beta_1 + \cdots + s_{m+r-1}\beta_{r-1} \pmod{\mathfrak{p}}.$$

Wäre nun die aus den Zahlen s_m gebildete Determinante E durch p teilbar, so könnte man nach dem in 1. bewiesenen Satze r ganze rationale Zahlen $x_0, x_1 \cdots x_{r-1}$, die nicht alle durch p teilbar sind, so wählen, daß

$$\left.\begin{array}{llll} s_0 & x_0 + s_1 x_1 + \cdots + s_{r-1} & x_{r-1} \equiv 0 \\ s_1 & x_0 + s_2 x_1 + \cdots + s_r & x_{r-1} \equiv 0 \\ \cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots \\ s_{r-1} & x_0 + s_r x_1 + \cdots + s_{2r-2} & x_{r-1} \equiv 0 \end{array}\right\} \pmod{p}$$

wird; dann würde

$$\eta_0(x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{r-1}\alpha^{r-1}) \equiv 0 \pmod{\mathfrak{p}},$$

und da der zweite Faktor nicht durch $\mathfrak{p}$ teilbar ist, so wäre

$$\eta_0 = s_0\beta_0 + s_1\beta_1 + \cdots + s_{r-1}\beta_{r-1} \equiv 0 \pmod{\mathfrak{p}};$$

allein es folgt aus (19) und (16), daß

$$\eta_0 = P'(\alpha)$$

und folglich nicht durch $\mathfrak{p}$ teilbar ist; mithin kann auch E, also auch R nicht durch p teilbar sein, w. z. b. w.

§ 6.

Die eben gewonnenen Resultate sind mehr als ausreichend, um auch den zweiten Teil unseres Satzes (§ 3) zu beweisen; derselbe läßt sich in folgender Weise aussprechen:

Geht p in der Grundzahl D des Körpers Ω auf, so ist p in diesem Körper durch das Quadrat eines Primideals teilbar.

In der Tat, wenn wir wieder mit $\omega_1, \omega_2 \cdots \omega_n$ eine Basis von $\mathfrak{o}$ bezeichnen, so ist die Grundzahl

$$D = \begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2) \cdots S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2\omega_2) \cdots S(\omega_2\omega_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1), & S(\omega_n\omega_2) \cdots S(\omega_n\omega_n) \end{vmatrix},$$

und wenn dieselbe durch die Primzahl p teilbar ist, so gibt es (zufolge § 5, 1.) n ganze rationale Zahlen $x_1, x_2 \cdots x_n$, welche die Kongruenzen

$$\left.\begin{array}{l} x_1 S(\omega_1\omega_1) + x_2 S(\omega_2\omega_1) + \cdots + x_n S(\omega_n\omega_1) \equiv 0 \\ x_1 S(\omega_1\omega_2) + x_2 S(\omega_2\omega_2) + \cdots + x_n S(\omega_n\omega_2) \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1 S(\omega_1\omega_n) + x_2 S(\omega_2\omega_n) + \cdots + x_n S(\omega_n\omega_n) \equiv 0 \end{array}\right\} \pmod{p}$$

befriedigen und nicht alle durch p teilbar sind; setzt man nun

$$\mu = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

so ist μ nicht teilbar durch p, und die vorstehenden Kongruenzen sind identisch mit den folgenden:

$$S(\mu\omega_1) \equiv 0,\ S(\mu\omega_2) \equiv 0 \cdots S(\mu\omega_n) \equiv 0 \pmod{p};$$

bezeichnet man mit $h_1, h_2 \cdots h_n$ beliebige ganze rationale Zahlen und setzt

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

so ist ω eine willkürliche Zahl in $\mathfrak{o}$, und die vorstehenden Kongruenzen lassen sich zusammenfassen in die folgende

$$S(\mu\omega) \equiv 0 \pmod{p};$$

bedeutet ω' ebenfalls eine willkürliche Zahl in $\mathfrak{o}$, so folgt hieraus auch

$$S(\mu\omega + p\omega') \equiv 0 \pmod{p}.$$

Der Inbegriff $\mathfrak{n}$ aller Zahlen ν von der Form $\mu\omega + p\omega'$ ist der größte gemeinschaftliche Teiler der beiden Hauptideale $\mathfrak{o}\mu, \mathfrak{o}p$, also ein Teiler von $\mathfrak{o}p$, und zwar ein echter (d. h. verschieden von $\mathfrak{o}p$), weil μ nicht durch p teilbar ist, und alle in diesem Ideal $\mathfrak{n}$ enthaltenen Zahlen ν genügen der Bedingung

$$S(\nu) \equiv 0 \pmod{p}.$$

Umgekehrt würde sich leicht zeigen lassen, daß hieraus die Teilbarkeit von D durch p folgt.

Nehmen wir nun an, unser Satz sei unrichtig, d. h. $\mathfrak{o}p$ sei ein Primideal oder ein Produkt von lauter verschiedenen Primidealen,

so muß es unter denselben wenigstens ein solches $\mathfrak{p}$ geben, welches in dem Ideal $\mathfrak{n}$ nicht aufgeht, weil sonst $\mathfrak{n}$ durch $\mathfrak{o}p$ teilbar wäre. Setzt man dann $\mathfrak{o}p = \mathfrak{p}\mathfrak{q}$, so muß $\mathfrak{q}$ durch $\mathfrak{n}$ teilbar, d. h. jede in $\mathfrak{q}$ enthaltene Zahl λ muß auch in $\mathfrak{n}$ enthalten sein, und folglich sind auch alle Spuren $S(\lambda)$ durch p teilbar. Dies steht aber im Widerspruch mit dem letzten Satze des vorigen Paragraphen; da nämlich nach unserer Annahme $\mathfrak{o}p$ nicht durch $\mathfrak{p}^2$, also $\mathfrak{q}$ nicht durch $\mathfrak{p}$ teilbar ist, so kann man (zufolge § 5, 5.) r Zahlen $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ aus $\mathfrak{q}$ so auswählen, daß die aus den Spuren $S(\varrho_i \varrho_{i'})$ gebildete Determinante R nicht durch p teilbar ist; da aber die Produkte $\varrho_i \varrho_{i'}$ ebenfalls in $\mathfrak{q}$ enthaltene Zahlen λ sind, deren Spuren folglich durch p teilbar sind, so müßte auch R durch p teilbar sein. Aus diesem Widerspruche folgt, daß unsere Annahme, $\mathfrak{o}p$ sei durch kein Primideal-Quadrat teilbar, unzulässig ist, und hiermit ist unser Satz bewiesen. —

Dieser Satz ist an sich von großem Interesse, und er gestattet zahlreiche wichtige Anwendungen; allein er gibt doch nur ein sehr unvollständiges Bild von der wirklichen Konstitution der Grundzahl D, die wir im folgenden viel genauer erforschen wollen; dabei wird sich von selbst ein neuer, von dem vorstehenden durchaus verschiedener Beweis des genannten Satzes ergeben.

§ 7.

Wir beginnen unsere neue Untersuchung mit einigen Betrachtungen, welche der allgemeinen Theorie der Moduln angehören (Z. § 165). Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, deren Zahlen wir resp. mit α, β bezeichnen wollen, so besteht ihr größter gemeinschaftlicher Teiler $\mathfrak{d}$ aus allen in der Form $\alpha + \beta$ darstellbaren Zahlen, und ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{m}$ ist der Inbegriff aller in $\mathfrak{a}$ und $\mathfrak{b}$ gleichzeitig enthaltenen Zahlen $\alpha = \beta$; diese beiden aus $\mathfrak{a}$ und $\mathfrak{b}$ abgeleiteten Moduln $\mathfrak{d}$ und $\mathfrak{m}$ werden wir in der Folge zur Abkürzung resp. mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ und $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnen*). Ist η eine bestimmte Zahl, so bedeutet $\mathfrak{a}\eta$ oder $\eta\mathfrak{a}$ den aus allen Produkten $\eta\alpha$ bestehenden Modul, und allgemein wird

*) Von derselben Bezeichnung habe ich in Ermangelung einer besseren auch früher schon Gebrauch gemacht in der Festschrift: Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig, 1877).

unter dem Produkt $\mathfrak{ab}$ der Modul verstanden, dessen Zahlen die Produkte $\alpha\beta$ oder Summen von solchen Produkten sind. Der Quotient

$$\frac{\mathfrak{b}}{\mathfrak{a}} \quad \text{oder} \quad \mathfrak{b}:\mathfrak{a}$$

soll den Inbegriff $\mathfrak{e}$ aller derjenigen Zahlen η bedeuten, für welche $\mathfrak{a}\eta$ durch $\mathfrak{b}$ teilbar wird; sind η', η'' solche Zahlen, so sind alle Produkte $\alpha\eta', \alpha\eta''$ in $\mathfrak{b}$ enthalten, und da $\mathfrak{b}$ ein Modul ist, so sind auch alle Produkte $\alpha(\eta' \pm \eta'')$ in $\mathfrak{b}$ enthalten, d. h. die beiden Moduln $\mathfrak{a}(\eta' \pm \eta'')$ sind ebenfalls teilbar durch $\mathfrak{b}$; mithin gehören die beiden Zahlen $(\eta' \pm \eta'')$ dem System $\mathfrak{e}$ an, welches folglich auch ein Modul ist. Offenbar ist das Produkt $\mathfrak{ae}$ durch $\mathfrak{b}$ teilbar; und wenn $\mathfrak{ac}$ durch $\mathfrak{b}$ teilbar ist, so ist der Modul $\mathfrak{c}$ durch den Quotient $\mathfrak{e}$ teilbar.

Unter der Ordnung $\mathfrak{a}^0$ des Moduls $\mathfrak{a}$ verstehen wir den Quotient

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}};$$

es leuchtet unmittelbar ein, erstens daß die Zahlen einer solchen Ordnung sich auch durch Multiplikation reproduzieren, und zweitens daß unter ihnen sich auch alle ganzen rationalen Zahlen befinden, daß also der Modul [1] durch $\mathfrak{a}^0$ teilbar ist; aus dieser letzteren Eigenschaft folgt, daß $\mathfrak{a}$ durch $\mathfrak{a}\mathfrak{a}^0$ teilbar ist, und da umgekehrt zufolge der Definition des Quotienten auch $\mathfrak{a}\mathfrak{a}^0$ durch $\mathfrak{a}$ teilbar ist, so ergibt sich der Satz

(1) $$\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a}.$$

Die angeführten beiden Eigenschaften von $\mathfrak{a}^0$ sind charakteristisch für jede Ordnung: ist $\mathfrak{n}$ ein Modul, dessen Zahlen sich auch durch Multiplikation reproduzieren, und ist der Modul [1] teilbar durch $\mathfrak{n}$, so ist $\mathfrak{n}$ gewiß eine Ordnung, nämlich die von $\mathfrak{n}$ selbst, d. h. es ist

(2) $$\mathfrak{n}^0 = \frac{\mathfrak{n}}{\mathfrak{n}} = \mathfrak{n};$$

die erste Eigenschaft besagt nämlich, daß $\mathfrak{n}^2$ durch $\mathfrak{n}$, mithin $\mathfrak{n}$ durch den Quotient $\mathfrak{n}^0$ teilbar ist, und da zufolge der zweiten Eigenschaft $\mathfrak{n}^0$ durch $\mathfrak{n}\mathfrak{n}^0$, also zufolge (1) durch $\mathfrak{n}$ teilbar ist, so ist $\mathfrak{n} = \mathfrak{n}^0$. Zugleich folgt aus (1), wenn $\mathfrak{a} = \mathfrak{n}$ gesetzt wird,

(3) $$\mathfrak{n}^2 = \mathfrak{n}.$$

Diese allgemeinen Betrachtungen wenden wir auf folgenden speziellen Fall an. Es sei Ω wieder ein endlicher Körper n^{ten} Grades,

und $\mathfrak{a}, \mathfrak{b}$ seien zwei endliche Moduln, deren Basen zugleich Basen von Ω sind; man überzeugt sich dann leicht, daß die Moduln

$$(4) \qquad \mathfrak{a}+\mathfrak{b}, \quad \mathfrak{a}-\mathfrak{b}, \quad \mathfrak{a}\mathfrak{b}, \quad \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{a}^0$$

von derselben Beschaffenheit sind. Ist nämlich

$$(5) \qquad \mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n], \quad \mathfrak{b} = [\beta_1, \beta_2 \cdots \beta_n],$$

so folgt

$$\mathfrak{a}+\mathfrak{b} = [\alpha_1, \alpha_2 \cdots \alpha_n, \beta_1, \beta_2 \cdots \beta_n],$$

und nach einem bekannten Satze (Z. § 165, S. 490) kann diese aus $2n$ Zahlen $\alpha_\iota, \beta_\iota$ bestehende Basis auf eine irreduktibele, aus n Zahlen bestehende reduziert werden. Da ferner jede Zahl des Körpers Ω, also auch jede Zahl in $\mathfrak{b}$ durch Multiplikation mit einem von Null verschiedenen rationalen Faktor in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so besitzt nach einem anderen Satze (Z. § 165, S. 486) auch $\mathfrak{a}-\mathfrak{b}$ eine aus n Zahlen bestehende, irreduktibele Basis. Für das Produkt und den Quotienten kann man dasselbe in ähnlicher Weise direkt dartun, aber wir ziehen es vor, diese Fälle auf die beiden vorigen durch folgenden Satz zurückzuführen:

Das Produkt $\mathfrak{a}\mathfrak{b}$ ist der größte gemeinschaftliche Teiler der Moduln

$$(6) \qquad \mathfrak{b}\alpha_1, \ \mathfrak{b}\alpha_2 \cdots \mathfrak{b}\alpha_n,$$

und der Quotient $\mathfrak{b}:\mathfrak{a}$ ist das kleinste gemeinschaftliche Vielfache der Moduln

$$(7) \qquad \mathfrak{b}\alpha_1^{-1}, \ \mathfrak{b}\alpha_2^{-1} \cdots \mathfrak{b}\alpha_n^{-1}.$$

Hiervon überzeugt man sich leicht; da nämlich jeder der Moduln (6) durch $\mathfrak{a}\mathfrak{b}$ teilbar ist, so gilt dasselbe von ihrem größten gemeinschaftlichen Teiler $\mathfrak{c}$; da ferner jedes Produkt $\alpha\beta$ von der Form $\beta\sum x_\iota\alpha_\iota$, also eine Summe von n Zahlen $(\beta x_\iota)\alpha_\iota$ ist, deren jede einem der n Moduln (6) angehört, so ist $\alpha\beta$ in $\mathfrak{c}$ enthalten, also $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{c}$, mithin $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. Da endlich eine Zahl η stets und nur dann dem Quotienten $\mathfrak{b}:\mathfrak{a}$ angehört, wenn die n Produkte $\eta\alpha_\iota$ in $\mathfrak{b}$, und folglich η in jedem der Moduln (7) enthalten ist, so ist dieser Quotient das kleinste gemeinschaftliche Vielfache der Moduln (7), w. z. b. w.

Nachdem unsere obige Behauptung über die aus $\mathfrak{a}, \mathfrak{b}$ abgeleiteten Moduln (4) hiermit gerechtfertigt ist, wollen wir zur Abkürzung festsetzen, daß unter einem Modul schlechthin und ebenso unter einer Ordnung immer nur ein solcher endlicher Modul verstanden werden soll, dessen Basis zugleich eine Basis des Körpers Ω bildet; nur

solche Moduln $\mathfrak{a}, \mathfrak{b} \cdots$ werden im weiteren Verlaufe unserer Untersuchung auftreten. In diesem Sinne gilt zunächst folgender Satz:

Ist $\mathfrak{b}$ teilbar durch $\mathfrak{a}$, so besteht der Quotient $\mathfrak{b} : \mathfrak{a}$ aus lauter ganzen Zahlen, d. h. er ist teilbar durch $\mathfrak{o}$.

Denn wenn η eine beliebige Zahl dieses Quotienten bedeutet, so sind die Produkte $\eta\alpha_1$, $\eta\alpha_2 \cdots \eta\alpha_n$ in $\mathfrak{b}$, also auch in $\mathfrak{a}$ enthalten, also von der Form $\sum x_\iota \alpha_\iota$, wo $x_1, x_2 \cdots x_n$ ganze rationale Zahlen sind, und hieraus folgt der Satz bekanntlich durch Elimination von $\alpha_1, \alpha_2 \cdots \alpha_n$.

Hieraus folgt von selbst, daß auch jede Ordnung $\mathfrak{a}^0$ oder $\mathfrak{n}$ durch die Ordnung $\mathfrak{o}$ teilbar ist; da ferner die Zahl 1 in $\mathfrak{n}$ enthalten ist, so leuchtet ein, daß

$$\mathfrak{n}\mathfrak{o} = \mathfrak{o} \tag{8}$$

ist. Aus der Teilbarkeit von $\mathfrak{n}$ durch $\mathfrak{o}$ folgt durch abermalige Anwendung desselben Satzes, daß der Quotient

$$\mathfrak{f} = \frac{\mathfrak{n}}{\mathfrak{o}}, \tag{9}$$

welchen wir (wie in § 3 der oben zitierten Festschrift) den **Führer der Ordnung** $\mathfrak{n}$ nennen wollen, ebenfalls durch $\mathfrak{o}$ teilbar ist. Da die Zahl 1 in $\mathfrak{o}$ enthalten, mithin $\mathfrak{f}$ durch $\mathfrak{f}\mathfrak{o}$ teilbar ist, so folgt aus (9), daß $\mathfrak{f}$ **durch** $\mathfrak{n}$ **teilbar** ist; da ferner $\mathfrak{o}^2 = \mathfrak{o}$, also das Produkt $(\mathfrak{f}\mathfrak{o})\mathfrak{o} = \mathfrak{f}\mathfrak{o}$ teilbar durch $\mathfrak{n}$ ist, so muß zufolge (9) auch der erste Faktor $\mathfrak{f}\mathfrak{o}$ durch den Quotienten $\mathfrak{f}$ teilbar sein, mithin ist

$$\mathfrak{f}\mathfrak{o} = \mathfrak{f}, \tag{10}$$

d. h. der Führer $\mathfrak{f}$ ist stets ein **Ideal***), und es leuchtet ein, daß **jedes** durch die Ordnung $\mathfrak{n}$ teilbare Ideal $\mathfrak{a}$ auch durch $\mathfrak{f}$ teilbar ist, weil das Produkt $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$, also durch $\mathfrak{n}$ teilbar ist. Offenbar ist $\mathfrak{o}$ selbst der Führer der Ordnung $\mathfrak{o}$.

§ 8.

Ein anderes wichtiges Hilfsmittel für die genaue Untersuchung der Grundzahl D gewinnen wir durch die folgenden Betrachtungen.

---

*) **Die erforderliche und hinreichende Bedingung, welche ein Ideal $\mathfrak{f}$ erfüllen muß, um Führer einer Ordnung $\mathfrak{n}$ sein zu können, besteht darin, daß, wenn $\mathfrak{p}$ irgend ein in $\mathfrak{f}$ aufgehendes Primideal ersten Grades, und $\mathfrak{f} = \mathfrak{p}\mathfrak{q}$ ist, jede durch das Ideal $\mathfrak{q}$ teilbare rationale Zahl auch durch $\mathfrak{f}$ teilbar ist; unter dieser Voraussetzung bildet das System aller derjenigen Zahlen, welche in bezug auf $\mathfrak{f}$ mit rationalen Zahlen kongruent sind, jedenfalls eine Ordnung $\mathfrak{n}$, deren Führer $\mathfrak{f}$ ist.**

1. Bilden die ganzen oder gebrochenen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$, deren Komplex wir im folgenden kurz durch $((\alpha_\iota))$ bezeichnen wollen, eine Basis des Körpers Ω, so ist bekanntlich ihre Diskriminante A von Null verschieden (Z. § 164, S. 477); da nun (zufolge § 1, (16)) diese Diskriminante

$$A = \begin{vmatrix} S(\alpha_1\alpha_1) \cdots S(\alpha_1\alpha_n) \\ \cdots\cdots\cdots\cdots \\ S(\alpha_n\alpha_1) \cdots S(\alpha_n\alpha_n) \end{vmatrix} \tag{1}$$

ist, so gibt es ein und nur ein System $((\alpha'_\iota))$ von n Zahlen $\alpha'_1, \alpha'_2 \cdots \alpha'_n$, welche den n Gleichungen

$$\alpha_r = \sum S(\alpha_r\alpha_\iota)\alpha'_\iota \tag{2}$$

genügen; diese n Zahlen gehören offenbar demselben Körper Ω an und bilden ebenfalls eine Basis von Ω, die wir das Komplement der Basis $((\alpha_\iota))$ nennen wollen. Bei dieser Ausdrucksweise ist wohl darauf zu achten, daß jeder bestimmten Zahl α_r der ersten Basis $((\alpha_\iota))$ eine bestimmte Zahl α'_r der komplementären Basis $((\alpha'_\iota))$ korrespondiert.

2. Ist ω eine beliebige Zahl des Körpers Ω, so sind die n Spuren $S(\omega\alpha_\iota)$ zugleich die Koordinaten von ω in bezug auf die Basis $((\alpha'_\iota))$, d. h. es ist

$$\omega = \sum S(\omega\alpha_\iota)\alpha'_\iota. \tag{3}$$

Da nämlich $((\alpha_\iota))$ eine Basis von Ω ist, so kann ω in die Form $\sum x_\iota\alpha_\iota$ gesetzt werden, wo die Koeffizienten x_ι rationale Zahlen sind, und offenbar folgt aus (2) unmittelbar die allgemeinere Gleichung (3).

3. Bezeichnet man durch das Symbol (r, s) den Wert 1 oder 0, je nachdem die der Reihe $1, 2 \cdots n$ angehörenden Indizes r, s gleich oder ungleich sind, so ist stets

$$S(\alpha_r\alpha'_s) = (r, s). \tag{4}$$

Dies ergibt sich unmittelbar aus (3), wenn man $\omega = \alpha'_s$ setzt.

4. Umgekehrt, wenn zwei Systeme $((\alpha_\iota))$ und $((\beta_\iota))$ den n^2 Relationen

$$S(\alpha_r\beta_s) = (r, s) \tag{5}$$

genügen, so bilden sie zwei Basen des Körpers, von denen jede das Komplement der anderen ist.

Denn zufolge (5) ist die aus den Spuren $S(\alpha_r\beta_s)$ gebildete Determinante $= 1$, also von Null verschieden, woraus (nach § 1, (15)) folgt, daß die Systeme $((\alpha_\iota))$ und $((\beta_\iota))$ Basen des Körpers sind, weil ihre Diskriminanten nicht verschwinden. Mithin besitzt $((\alpha_\iota))$ eine komplementäre Basis $((\alpha'_\iota))$, und da aus (3) und (5)

$$\beta_s = \sum S(\beta_s\alpha_\iota)\alpha'_\iota = \sum (s, \iota)\alpha'_\iota = \alpha'_s$$

folgt, so ist $((\alpha_i'))$ identisch mit $((\beta_i))$. Da ferner die Relationen (5) durchaus symmetrisch in bezug auf beide Systeme sind, so ist ebenso $((\alpha_i))$ das Komplement von $((\beta_i))$. Es ergibt sich daher auch der Satz:

5. Ist $((\alpha_i'))$ das Komplement der Basis $((\alpha_i))$, so ist $((\alpha_i))$ dasjenige von $((\alpha_i'))$. Es gehören daher immer zwei Basen zu einem Paar komplementärer Basen zusammen, und folglich gilt für jede Zahl ω auch die Gleichung

$$\omega = \sum S(\omega \alpha_i') \alpha_i. \tag{6}$$

6. Wenn zwei Systeme $((\alpha_i))$, $((\beta_i))$ die Eigenschaft haben, daß für jede Zahl ω die Gleichung

$$\omega = \sum S(\omega \alpha_i) \beta_i \tag{7}$$

gilt, so bilden sie ein Paar komplementärer Basen.

Denn daraus, daß jede Zahl ω des Körpers in der vorstehenden Form (7) darstellbar ist, folgt zunächst, daß das System $((\beta_i))$ eine Basis von Ω ist; und wenn man $\omega = \beta_s$ setzt, so folgen hieraus ferner die Relationen (5).

7. Bezeichnen wir immer mit $((\alpha_i'))$ das Komplement der Basis $((\alpha_i))$, so ist

$$\sum \alpha_i \alpha_i' = 1. \tag{8}$$

Denn wenn man ω in (3) durch $\omega \alpha_s'$ ersetzt, so erhält man

$$\omega \alpha_s' = \sum S(\omega \alpha_i' \alpha_s') \alpha_i';$$

hieraus folgt (nach § 1, (11))

$$S(\omega) = \sum S(\omega \alpha_i \alpha_i') = S\left(\omega \sum \alpha_i \alpha_i'\right),$$

woraus unser Satz sich ergibt (zufolge § 1, (17) und (18)).

8. Der Koeffizient, welchen das Element $\alpha_m^{(r)}$ in der Determinante

$$\sum \pm \alpha_1^{(1)} \alpha_2^{(2)} \cdots \alpha_n^{(n)} = \sqrt{A} \tag{9}$$

hat, ist

$$= \alpha_m'^{(r)} \sqrt{A}, \tag{10}$$

und folglich ist auch

$$\sum \alpha_i^{(r)} \alpha_i'^{(s)} = (r, s). \tag{11}$$

In diesem Satze, welcher ohne weiteres aus (4) und bekannten Determinantensätzen folgt, ist der vorige Satz als spezieller Fall enthalten.

9. Ist η von Null verschieden, so sind die Basen $((\eta \alpha_i))$ und $((\eta^{-1} \alpha_i'))$ komplementär.

Dies folgt sofort aus den obigen Sätzen 3. und 4., oder auch aus Gleichung (3), wenn man ω durch $\omega\eta$ ersetzt, durch η dividiert, und den Satz 6. zuzieht.

10. Sind zwei Basen $((\alpha_\iota))$, $((\beta_\iota))$ durch die n Gleichungen

$$\alpha_r = \sum c_{r,\iota}\beta_\iota \tag{12}$$

mit rationalen Koeffizienten $c_{r,s}$ verbunden, so gelten für ihre Komplemente $((\alpha'_\iota))$, $((\beta'_\iota))$ die n Gleichungen

$$\beta'_s = \sum c_{\iota,s}\alpha'_\iota. \tag{13}$$

Denn zufolge (12) und (6) ist $c_{r,s} = S(\alpha_r\beta'_s)$, und hieraus folgt (13) vermöge (3).

11. Die Potenzen $1, \theta, \theta^2 \cdots \theta^{n-1}$ bilden bekanntlich eine Basis des Körpers, wenn die zugehörige Gleichung n^{ten} Grades

$$F(\theta) = 0 \tag{14}$$

irreduktibel ist, d. h. wenn die Zahl

$$\theta^* = F'(\theta) \tag{15}$$

von Null verschieden ist (§ 1); unter dieser Voraussetzung stellen wir uns die Aufgabe, die komplementäre Basis zu finden.

Jede Zahl ω des Körpers läßt sich in der Form $\omega = \psi(\theta)$ darstellen, wo $\psi(t)$ eine ganze Funktion bedeutet, deren Grad $< n$ ist, und deren Koeffizienten rationale Zahlen sind; dann ist bekanntlich

$$\psi(t) = \frac{\psi(\theta^{(1)})}{F'(\theta^{(1)})}\cdot\frac{F(t)}{t-\theta^{(1)}} + \cdots + \frac{\psi(\theta^{(n)})}{F'(\theta^{(n)})}\cdot\frac{F(t)}{t-\theta^{(n)}};$$

setzt man nun die ganze Funktion $(n-1)^{\text{ten}}$ Grades

$$\frac{F(t)}{t-\theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1}t^{n-1} = \sum \eta_s t^s, \tag{16}$$

so nimmt diese Gleichung folgende Form an:

$$\psi(t) = \sum S\left(\frac{\omega\eta_s}{\theta^*}\right)t^s,$$

und folglich ist

$$\omega = \sum S\left(\frac{\omega\eta_s}{\theta^*}\right)\theta^s.$$

Hieraus ergibt sich nach dem Satze 6., daß die Systeme

$$\left(\left(\frac{\eta_s}{\theta^*}\right)\right) \text{ und } ((\theta^s)) \tag{17}$$

komplementär sind. Setzt man (wie in § 1, (1))

$$F(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n, \tag{18}$$

so ergeben sich für die durch (16) definierten Zahlen η_s folgende Ausdrücke (vgl. § 5, (19)):

$$(19)\quad \begin{cases} \eta_0 &= \theta^{n-1} + a_1\theta^{n-2} + \cdots + a_{n-2}\theta + a_{n-1} \\ \eta_1 &= \theta^{n-2} + a_1\theta^{n-3} + \cdots + a_{n-2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{n-2} &= \theta + a_1 \\ \eta_{n-1} &= 1. \end{cases}$$

§ 9.

Wir verbinden nun die in den beiden vorhergehenden Paragraphen gewonnenen Resultate miteinander, wobei, wie wir nochmals bemerken, unter einem **Modul** stets ein solcher endlicher Modul zu verstehen ist, dessen Basis zugleich eine Basis des Körpers Ω bildet.

1. Die beiden Systeme $((\alpha_i))$ und $((\beta_i))$ bilden bekanntlich stets und nur dann Basen eines und desselben Moduls $\mathfrak{a}$, wenn sie durch n Gleichungen von der Form

$$\alpha_r = \sum c_{r,i}\beta_i$$

miteinander verbunden sind, wo die Koeffizienten $c_{r,s}$ ganze rationale Zahlen bedeuten, deren Determinante

$$\sum \pm c_{1,1}\, c_{2,2} \cdots c_{n,n} = \pm 1$$

ist (Z. § 165, S. 489). Da nun (nach § 8, (13)) die zugehörigen komplementären Basen $((\alpha_i'))$ und $((\beta_i'))$ durch die Gleichungen

$$\beta_s' = \sum c_{i,s}\alpha_i'$$

miteinander verbunden sind, so bilden sie ebenfalls Basen eines und desselben Moduls, welcher mithin durch den Modul $\mathfrak{a}$ allein schon vollständig bestimmt und von der Wahl der Basis $((\alpha_i))$ oder $((\beta_i))$ gänzlich unabhängig ist; dieser Modul soll das **Komplement** von $\mathfrak{a}$ heißen und immer mit $\mathfrak{a}'$ bezeichnet werden. Da ferner (nach § 8, 5.) umgekehrt $((\alpha_i))$ die komplementäre Basis von $((\alpha_i'))$ ist, so ergibt sich, daß der Modul $\mathfrak{a}$ das Komplement des Moduls $\mathfrak{a}'$ ist, was wir durch die Gleichung

$$(1)\qquad (\mathfrak{a}')' = \mathfrak{a}$$

ausdrücken.

2. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so ist $\mathfrak{b}'$ teilbar durch $\mathfrak{a}'$, und zugleich ist $(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', \mathfrak{b}')$.

Denn die Basen $((\alpha_i))$ und $((\beta_i))$ der beiden Moduln $\mathfrak{a}$ und $\mathfrak{b}$ sind durch $2n$ Gleichungen von der Form

$$\alpha_r = \sum c_{r,i}\beta_i, \quad \beta_s' = \sum c_{i,s}\alpha_i'$$

verbunden, wo die Koeffizienten $c_{r,s}$ ganze rationale Zahlen sind, und der absolute Wert der aus ihnen gebildeten Determinante ist nach einem bekannten Satze (Z. § 165, S. 493) sowohl $= (\mathfrak{b}, \mathfrak{a})$ als $= (\mathfrak{a}', \mathfrak{b}')$.

3. Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so ist

$$(2) \qquad (\mathfrak{a}+\mathfrak{b})' = \mathfrak{a}' - \mathfrak{b}'; \quad (\mathfrak{a}-\mathfrak{b})' = \mathfrak{a}' + \mathfrak{b}'.$$

Da nämlich $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{a}+\mathfrak{b}$ teilbar sind, so ist (nach 2.) umgekehrt $(\mathfrak{a}+\mathfrak{b})'$ durch $\mathfrak{a}'$ und $\mathfrak{b}'$, also auch durch $\mathfrak{a}' - \mathfrak{b}'$ teilbar. Umgekehrt, da $\mathfrak{a}' - \mathfrak{b}'$ durch $\mathfrak{a}'$ und $\mathfrak{b}'$ teilbar ist, so sind (nach 2.) die Moduln $\mathfrak{a}$ und $\mathfrak{b}$, also auch $\mathfrak{a}+\mathfrak{b}$ durch $(\mathfrak{a}'-\mathfrak{b}')'$ teilbar, woraus wieder (nach 2. und (1)) folgt, daß $\mathfrak{a}'-\mathfrak{b}'$ durch $(\mathfrak{a}+\mathfrak{b})'$ teilbar ist. Aus dieser gegenseitigen Teilbarkeit der beiden Moduln $(\mathfrak{a}+\mathfrak{b})'$ und $\mathfrak{a}'-\mathfrak{b}'$ folgt aber ihre Identität; der zweite Satz (2) ist identisch mit diesem ersten, wie man leicht erkennt, wenn man $\mathfrak{a}, \mathfrak{b}$ resp. durch $\mathfrak{a}', \mathfrak{b}'$ ersetzt und den Satz (1) zuzieht.

4. Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so ist

$$(3) \qquad (\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', \mathfrak{b}').$$

Denn nach allgemeinen Sätzen (Z. § 165, S. 484) ist

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}+\mathfrak{b}, \mathfrak{a}); \quad (\mathfrak{a}', \mathfrak{b}') = (\mathfrak{a}', \mathfrak{a}'-\mathfrak{b}'),$$

und da $\mathfrak{a}$ teilbar durch $\mathfrak{a}+\mathfrak{b}$ ist, so folgt aus den Sätzen 2. und 3., daß

$$(\mathfrak{a}+\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', (\mathfrak{a}+\mathfrak{b})') = (\mathfrak{a}', \mathfrak{a}'-\mathfrak{b}')$$

ist, w. z. b. w.

5. Ist η eine von Null verschiedene Zahl des Körpers Ω, so ist

$$(4) \qquad (\mathfrak{a}\eta)' = \mathfrak{a}'\eta^{-1}.$$

Dies folgt ohne weiteres aus dem Satze 9. in § 8.

6. Mit Zuziehung der komplementären Moduln lassen sich die beiden Operationen der Multiplikation und Division der Moduln aufeinander zurückführen:

$$(5) \qquad (\mathfrak{a}\mathfrak{b})' = \frac{\mathfrak{b}'}{\mathfrak{a}} = \frac{\mathfrak{a}'}{\mathfrak{b}}; \qquad \mathfrak{a}\mathfrak{b} = \left(\frac{\mathfrak{b}'}{\mathfrak{a}}\right)' = \left(\frac{\mathfrak{a}'}{\mathfrak{b}}\right)'.$$

Da nämlich, wenn $((\alpha_i))$ eine Basis von $\mathfrak{a}$ bedeutet, das Produkt $\mathfrak{a}\mathfrak{b}$ (zufolge § 7, (6)) der größte gemeinschaftliche Teiler der Moduln

$$\mathfrak{b}\alpha_1, \quad \mathfrak{b}\alpha_2 \cdots \mathfrak{b}\alpha_n$$

ist, so folgt (aus 3.), daß das Komplement $(\mathfrak{a}\mathfrak{b})'$ das kleinste gemeinschaftliche Vielfache der Komplemente

$$(\mathfrak{b}\alpha_1)', \quad (\mathfrak{b}\alpha_2)' \cdots (\mathfrak{b}\alpha_n)'$$

ist; da diese letzteren (zufolge 5.) mit

$$\mathfrak{b}'\alpha_1^{-1}, \quad \mathfrak{b}'\alpha_2^{-1} \cdots \mathfrak{b}'\alpha_n^{-1}$$

identisch sind, so folgt (nach § 7, (7)), daß $(\mathfrak{a}\mathfrak{b})'$ zugleich der Quotient $\mathfrak{b}' : \mathfrak{a}$ ist. Hiermit ist unser Satz vollständig bewiesen; es wird aber dem Leser vielleicht willkommen sein, wenn wir noch den folgenden, auf Rechnung gegründeten Beweis hinzufügen.

Ist $((\beta_\iota))$ eine Basis von $\mathfrak{b}$, so bilden die n^2 Produkte $\alpha_r \beta_s$ eine Basis des Produktes $\mathfrak{a}\mathfrak{b}$, welche sich nach allgemeinen Sätzen (Z. § 165) auf eine irreduktibele Basis $((\gamma_\iota))$ zurückführen läßt; es gelten dann n^3 Gleichungen von der Form

$$\alpha_r \beta_s = \sum p_\iota^{r,s} \gamma_\iota \tag{6}$$

und umgekehrt n Gleichungen von der Form

$$\gamma_m = \sum q_m^{\iota,\iota'} \alpha_\iota \beta_{\iota'}, \tag{7}$$

wo alle Koeffizienten $p_m^{r,s}$ und $q_m^{r,s}$ ganze rationale Zahlen sind; substituiert man in (7) für die Produkte $\alpha_\iota \beta_{\iota'}$ ihre Ausdrücke gemäß (6), so folgt aus der Irreduktibilität der Basis $((\gamma_\iota))$, daß die Summe

$$\sum p_h^{\iota,\iota'} q_m^{\iota,\iota'} = (h, m), \tag{8}$$

d. h. $= 1$ oder $= 0$ ist, je nachdem h, m gleich oder ungleich sind. Da nun zwischen den Basen $((\alpha_r \beta_\iota))$ und $((\gamma_\iota))$ der Moduln $\mathfrak{b}\alpha_r$ und $\mathfrak{a}\mathfrak{b}$ diejenigen n linearen Relationen (6) stattfinden, in denen r einen und denselben Wert behauptet, so folgen (nach den Sätzen 9. und 10. in § 8) durch den Übergang zu den Komplementen $\mathfrak{b}'\alpha_r^{-1}$ und $(\mathfrak{a}\mathfrak{b})'$ die Gleichungen*)

$$\alpha_r \gamma'_m = \sum p_m^{r,\iota} \beta'_\iota; \tag{9}$$

mithin ist das Produkt $\mathfrak{a}(\mathfrak{a}\mathfrak{b})'$ teilbar durch $\mathfrak{b}'$, also $(\mathfrak{a}\mathfrak{b})'$ teilbar durch den Quotient $\mathfrak{b}' : \mathfrak{a}$. Umgekehrt, wenn η eine beliebige Zahl dieses Quotienten bedeutet, also $\mathfrak{a}\eta$ durch $\mathfrak{b}'$ teilbar ist, so gelten n Gleichungen von der Form

$$\eta \alpha_r = \sum c^{r,\iota} \beta'_\iota, \tag{10}$$

wo die Koeffizienten $c^{r,s}$ ebenfalls ganze rationale Zahlen sind; setzt man ferner

$$e_m = S(\eta \gamma_m), \quad \text{also} \quad \eta = \sum e_\iota \gamma'_\iota, \tag{11}$$

so folgt mit Rücksicht auf (9) die Gleichung

$$\eta \alpha_r = \sum e_\iota \alpha_r \gamma'_\iota = \sum e_\iota p_\iota^{r,\iota'} \beta'_{\iota'};$$

vergleicht man dies mit (10), so folgt

$$c^{r,s} = \sum e_\iota p_\iota^{r,s};$$

*) Dies ergibt sich noch einfacher durch die Bemerkung, daß $p_m^{r,s} = S(\alpha_r \beta_s \gamma'_m)$ ist.

multipliziert man jetzt mit $q_m^{r,s}$ und summiert über alle Werte von r, s, so ergibt sich mit Rücksicht auf (8)

$$e_m = \sum c^{i,i'} q_m^{i,i'};$$

mithin sind die Zahlen e_m ebenfalls ganze Zahlen, woraus nach (11) folgt, daß η in $(\mathfrak{a}\mathfrak{b})'$ enthalten ist. Also ist der Quotient $\mathfrak{b}' : \mathfrak{a}$ teilbar durch $(\mathfrak{a}\mathfrak{b})'$, und aus dieser gegenseitigen Teilbarkeit beider Moduln folgt ihre Identität, w. z. b. w.

7. Je zwei komplementäre Moduln $\mathfrak{a}, \mathfrak{a}'$ haben dieselbe Ordnung.

Denn setzt man in dem vorigen Satze $\mathfrak{b} = \mathfrak{a}'$, also $\mathfrak{b}' = \mathfrak{a}$, so folgt

$$(\mathfrak{a}\mathfrak{a}')' = \mathfrak{a}^0 = (\mathfrak{a}')^0. \tag{12}$$

8. Ist θ eine ganze Zahl, und zwar Wurzel einer irreduktibelen Gleichung n^{ten} Grades $F(\theta) = 0$, also $\theta^* = F'(\theta)$ von Null verschieden, so ist der Modul

$$\mathfrak{n} = [1, \theta, \theta^2 \cdots \theta^{n-1}] \tag{13}$$

offenbar eine Ordnung, und solche Ordnungen wollen wir reguläre Ordnungen nennen. Durch den Übergang zum Komplement erhält man

$$\theta^* \mathfrak{n}' = [\eta_0, \eta_1 \cdots \eta_{n-1}],$$

wo die Zahlen $\eta_0, \eta_1 \cdots \eta_{n-1}$ durch die Gleichungen (19) in § 8 definiert sind; da nun in unserem Falle, wo θ eine ganze Zahl ist, die Koeffizienten $1, a_1, a_2 \cdots a_n$ der Funktion $F(t)$ ganze rationale Zahlen sind, so bilden offenbar die Zahlen $\eta_0, \eta_1 \cdots \eta_{n-1}$ ebenfalls eine Basis von $\mathfrak{n}$, und folglich ist

$$\theta^* \mathfrak{n}' = \mathfrak{n}. \tag{14}$$

Hieraus folgt durch Multiplikation mit $\mathfrak{o}$ nach dem Satze (8) in § 7

$$\theta^* \mathfrak{o}\mathfrak{n}' = \mathfrak{o},$$

und hieraus (nach dem obigen Satze 5.)

$$(\mathfrak{o}\mathfrak{n}')' = \theta^* \mathfrak{o}'.$$

Bezeichnen wir nun wieder mit $\mathfrak{f}$ den Führer der Ordnung $\mathfrak{n}$ (§ 7, (9)), so ist (nach dem obigen Satze 6.)

$$\mathfrak{f} = \frac{\mathfrak{n}}{\mathfrak{o}} = (\mathfrak{o}'\mathfrak{n}')',$$

mithin

$$\mathfrak{f} = \theta^* \mathfrak{o}'. \tag{15}$$

Bedeutet ferner k wieder den Index der Zahl θ (§ 2), so ist nach (14), (15) und früheren Sätzen

$$k = (\mathfrak{o}, \mathfrak{n}) = (\mathfrak{n}', \mathfrak{o}') = (\theta^* \mathfrak{n}', \theta^* \mathfrak{o}') = (\mathfrak{n}, \mathfrak{f}),$$

und da $\mathfrak{k}$ durch $\mathfrak{n}$, ferner $\mathfrak{n}$ durch $\mathfrak{o}$ teilbar ist, so folgt

$$(\mathfrak{o}, \mathfrak{k}) = (\mathfrak{o}, \mathfrak{n})(\mathfrak{n}, \mathfrak{k}),$$

mithin

$$N(\mathfrak{k}) = k^2. \tag{16}$$

Da endlich jede Zahl in $\mathfrak{o}$ durch Multiplikation mit k in eine Zahl der Ordnung $\mathfrak{n}$ verwandelt wird (Z. § 165, S. 485), so ist das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{n}$, folglich auch durch den Führer $\mathfrak{k}$ teilbar (§ 7); mithin gibt es ein und nur ein Ideal $\mathfrak{k}_1$, welches der Bedingung

$$\mathfrak{o}\mathfrak{k} = \mathfrak{k}\mathfrak{k}_1 \tag{17}$$

genügt, und hieraus folgt

$$N(\mathfrak{k}_1) = k^{n-2}. \tag{18}$$

§ 10.

Bezeichnen wir mit $((\omega_\iota))$ eine Basis von $\mathfrak{o}$, mit $((\omega'_\iota))$ die entsprechende Basis des Komplements $\mathfrak{o}'$, so gelten die n Gleichungen

$$\omega_\tau = \sum S(\omega_\tau \omega_\iota)\, \omega'_\iota, \tag{1}$$

und da die Spuren der ganzen Zahlen $\omega_\tau \omega_\sigma$ auch ganze Zahlen sind, so ist $\mathfrak{o}$ teilbar durch $\mathfrak{o}'$; da ferner die Grundzahl

$$D = \begin{vmatrix} S(\omega_1\omega_1) \cdots S(\omega_1\omega_n) \\ \cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1) \cdots S(\omega_n\omega_n) \end{vmatrix} \tag{2}$$

ist, so folgt (Z. § 165, S. 493), daß ihr absoluter Wert

$$(D) = (\mathfrak{o}', \mathfrak{o}) \tag{3}$$

ist, und zugleich leuchtet ein, daß der Modul $D\mathfrak{o}'$ teilbar durch $\mathfrak{o}$ ist. Das Komplement $\mathfrak{o}'$ hat (nach § 9, 7.) dieselbe Ordnung $\mathfrak{o}$, wie $\mathfrak{o}$ selbst; mithin ist $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}'$, also auch $\mathfrak{o}(D\mathfrak{o}') = D\mathfrak{o}'$, und folglich ist der Modul $D\mathfrak{o}'$ ein Ideal. Da ferner, wie schon oben bemerkt, $\mathfrak{o}$ durch $\mathfrak{o}'$ teilbar ist, so ist das Hauptideal $D\mathfrak{o}$ auch teilbar durch das Ideal $D\mathfrak{o}'$, und folglich gibt es ein und nur ein Ideal $\mathfrak{d}$, welches der Bedingung

$$D\mathfrak{o} = \mathfrak{d}(D\mathfrak{o}'), \qquad \mathfrak{o} = \mathfrak{d}\mathfrak{o}' \tag{4}$$

genügt; dieses Ideal $\mathfrak{d}$ wollen wir das Grundideal des Körpers Ω nennen. Aus (3) und einem bekannten Satze der Idealtheorie (Z. § 173, 7.) folgt nun

$$(D) = (D\mathfrak{o}', D\mathfrak{o}) = (D\mathfrak{o}', \mathfrak{d}D\mathfrak{o}') = (\mathfrak{o}, \mathfrak{d}),$$

also erhalten wir den Fundamentalsatz:

$$N(\mathfrak{d}) = (D) \tag{5}$$

die Grundzahl eines Körpers ist, absolut genommen, immer die Norm seines Grundideals.

Betrachten wir nun die aus den konjugierten Zahlen $\omega_r^{(s)}$ gebildete Determinante

$$\sum \pm \omega_1^{(1)} \omega_2^{(2)} \cdots \omega_n^{(n)} = \sqrt{D}, \tag{6}$$

so ist $\omega_r' \sqrt{D}$ (nach § 8, 8.) der Koeffizient des Elements ω_r, mithin eine ganze Zahl, weil alle diese Koeffizienten durch Addition, Subtraktion und Multiplikation aus den Elementen $\omega_r^{(s)}$ gebildet werden, welche in unserem Falle ganze algebraische Zahlen sind. Hieraus folgt weiter, daß alle Produkte $D\omega_r'\omega_s'$ aus zwei solchen Zahlen $\omega_r' \sqrt{D}$ und $\omega_s' \sqrt{D}$ ebenfalls ganze Zahlen, mithin in $\mathfrak{o}$ enthalten sind; diese Produkte bilden aber eine (reduktibele) Basis des Moduls

$$D\mathfrak{o}'\mathfrak{o}' = \mathfrak{d}_1, \tag{7}$$

welcher mithin teilbar durch $\mathfrak{o}$ ist. Da ferner, wie schon bemerkt, $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}'$ ist, so folgt $\mathfrak{o}\mathfrak{d}_1 = \mathfrak{d}_1$, mithin ist $\mathfrak{d}_1$ ein Ideal. Multipliziert man nun die Gleichung (4) mit $\mathfrak{o}'$, so folgt

$$D\mathfrak{o}' = \mathfrak{d}\mathfrak{d}_1, \tag{8}$$

also auch

$$D\mathfrak{o} = \mathfrak{d}^2\mathfrak{d}_1. \tag{9}$$

Die Grundzahl D ist daher stets teilbar durch das Quadrat des Grundideals $\mathfrak{d}$, und zugleich ist

$$N(\mathfrak{d}_1) = (D)^{n-2}. \tag{10}$$

Nachdem durch den Satz (5) die Bestimmung der Grundzahl eines Körpers auf diejenige seines Grundideals zurückgeführt ist leuchtet ein, wie wichtig es ist, die Konstitution des letzteren, d. h. seine Zusammensetzung aus Primidealen genau zu erforschen. Für diese Untersuchung, welche in den folgenden Paragraphen ausgeführt werden soll, ist die Betrachtung der regulären Ordnungen erforderlich, und hierzu geben auch die am Schlusse des vorhergehenden Paragraphen gewonnenen Resultate die natürlichste Veranlassung. In der Tat, wenn man dieselben Bezeichnungen beibehält und die dortige Gleichung (15) mit $\mathfrak{d}$ multipliziert, so ergibt sich mit Rücksicht auf die obige Gleichung (4) der wichtige Satz:

$$\mathfrak{o}\theta^* = \mathfrak{d}\mathfrak{k}. \tag{11}$$

Nimmt man die Norm, so erhält man von neuem das schon (aus § 2, (4)) bekannte Resultat

$$N(\theta^*) = \pm D k^2, \tag{12}$$

wo k wieder den Index der Zahl θ bedeutet; da ferner $\mathfrak{o}k = \mathfrak{k}\mathfrak{k}_1$ ist, so folgt mit Rücksicht auf (9)

$$\mathfrak{o}N(\theta^*) = \mathfrak{d}^2\mathfrak{d}_1\mathfrak{k}^2\mathfrak{k}_1^2,$$

also zufolge (11)

$$\mathfrak{o}N(\theta^*) = \theta^*\theta^* \cdot \mathfrak{d}_1\mathfrak{k}_1^2, \tag{13}$$

mithin ist $N(\theta^*)$ stets durch das Quadrat von θ^* teilbar, ein Satz, der auch unmittelbar aus der Definition von θ^* leicht abzuleiten ist.

Aber diese letzten Bemerkungen sind nur von sehr untergeordneter Bedeutung im Vergleich mit dem äußerst wichtigen Satze, welcher in der Gleichung (11) enthalten ist. Das Grundideal $\mathfrak{d}$ ist demnach ein fester gemeinschaftlicher Teiler aller Zahlen θ^*, die allen ganzen Zahlen θ entsprechen, während der andere Faktor $\mathfrak{k}$ von θ abhängig, nämlich der Führer der durch θ erzeugten regulären Ordnung $\mathfrak{n}$ ist; wenn zwei Zahlen θ dieselbe Ordnung $\mathfrak{n}$ erzeugen, so werden folglich die ihnen entsprechenden beiden Zahlen θ^* assoziiert, d. h. ihr Quotient wird eine Einheit sein. Wenn $\mathfrak{o}$ selbst eine reguläre Ordnung ist, wie es z. B. bei jedem quadratischen Körper und auch bei jedem Körper geschieht, der aus einer Gleichung von der Form $\theta^m = 1$ entspringt, so reicht der genannte Satz allein schon aus, um die Konstitution des Grundideals $\mathfrak{d}$ und der Grundzahl D zu bestimmen, weil dann $\mathfrak{o}\theta^* = \mathfrak{d}$ wird. Aber diese Fälle bilden doch nur Ausnahmen unter der unendlichen Mannigfaltigkeit der Körper, und es bedarf daher, um zu unserem Ziele zu gelangen, einer genauen Untersuchung der regulären Ordnungen. Während wir in der früheren Abhandlung (G. § 5) nachgewiesen haben, daß es Körper gibt, in welchen die Indizes k aller Zahlen θ durch eine und dieselbe Primzahl p teilbar sind, so werden wir jetzt zeigen, daß die Führer $\mathfrak{k}$ der entsprechenden regulären Ordnungen $\mathfrak{n}$ niemals alle durch ein und dasselbe Primideal $\mathfrak{p}$ teilbar sind, woraus nach (11) folgt, daß das Grundideal $\mathfrak{d}$ der größte gemeinschaftliche Teiler aller Hauptideale von der Form $\mathfrak{o}\theta^*$ ist.

§ 11.

Um diesen Nachweis zu liefern, benutzen wir die Theorie der höheren Kongruenzen, und um keine Lücken zu lassen, schicken wir, auf die Gefahr hin Bekanntes zu wiederholen, einige Bemerkungen über den Zusammenhang zwischen Zahlenkongruenzen und Funktionenkongruenzen voraus, bei denen es sich immer nur um ganze Funktionen

einer Variablen t handelt, deren Koeffizienten ganze rationale Zahlen sind.

Es sei $\mathfrak{p}$ ein bestimmtes Primideal im Körper Ω, und p die durch $\mathfrak{p}$ teilbare positive rationale Primzahl. Wenn nun θ irgend eine ganze Zahl des Körpers, und $F(t)$ wieder die zugehörige Funktion n^{ten} Grades bedeutet (§ 1), so kann man die letztere in bezug auf den Modul p in Primfunktionen $P(t)$ zerlegen, deren höchste Koeffizienten wir immer $= 1$ annehmen (K. § 6); aus dieser Zerlegung

$$F(t) \equiv \Pi P(t) \pmod{p} \tag{1}$$

folgt, weil $F(\theta) = 0$ ist, die Zahlenkongruenz

$$\Pi P(\theta) \equiv 0 \pmod{p}, \tag{2}$$

mithin muß einer der Faktoren, den wir mit $P(\theta)$ bezeichnen wollen, durch das in p aufgehende Primideal $\mathfrak{p}$ teilbar sein, also

$$P(\theta) \equiv 0 \pmod{\mathfrak{p}}. \tag{3}$$

Da eine beliebige Funktion $\psi(t)$ entweder durch $P(t)$ teilbar oder relative Primfunktion zu $P(t)$ ist (mod. p), und da im letzteren Falle eine Kongruenz von der Form

$$\psi(t)\psi_1(t) + P(t)\psi_2(t) \equiv 1 \pmod{p} \tag{4}$$

stattfindet (K. § 4), so leuchtet ein, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}} \tag{5}$$

durchaus gleichbedeutend mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p,\ P(t)} \tag{5'}$$

ist (K. § 7). Hieraus folgt einerseits, daß die Primfunktion $P(t)$, deren Grad wir mit f bezeichnen wollen, durch die Zahl θ, für welche die Kongruenz (3) gelten soll, vollständig bestimmt ist (mod. p); man würde auch — was aber hier kein weiteres Interesse hat — leicht finden, daß allen und nur denjenigen Zahlen, welche mit einer der f inkongruenten Zahlen

$$\theta,\ \theta^p,\ \theta^{p^2} \dots \theta^{p^{f-1}}$$

nach $\mathfrak{p}$ kongruent sind, dieselbe Primfunktion $P(t)$ entspricht, und daß f ein Divisor vom Grade des Primideals $\mathfrak{p}$ ist. Andererseits ergibt sich aus der Äquivalenz von (5) und (5'), daß zwei ganze Zahlen von der Form $\psi_1(\theta)$, $\psi_2(\theta)$ stets und nur dann nach $\mathfrak{p}$ kongruent sind, wenn die Funktionen $\psi_1(t)$, $\psi_2(t)$ nach dem Doppelmodul p, $P(t)$ kongruent sind, und da p^f die genaue Anzahl aller nach diesem Doppelmodul inkongruenten Funktionen $\psi(t)$ ist (K. § 8), so

ist p^f zugleich die Anzahl aller nach $\mathfrak{p}$ inkongruenten Zahlen von der Form $\psi(\theta)$.

Ist daher die Zahl θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades $F(\theta) = 0$, ist also die entsprechende Zahl $\theta^* = F'(\theta)$ von Null verschieden, so wird, wenn wir wieder die durch θ erzeugte reguläre Ordnung

$$[1,\ \theta,\ \theta^2 \cdots \theta^{n-1}] = \mathfrak{n} \tag{6}$$

setzen,

$$(\mathfrak{n}, \mathfrak{p}) = p^f. \tag{7}$$

Unter dieser Voraussetzung gilt nun, wenn wir zur Abkürzung

$$P(\theta) = \varrho \tag{8}$$

setzen und mit $\mathfrak{k}$ den Führer der Ordnung $\mathfrak{n}$ bezeichnen, der folgende wichtige Satz:

Die erforderlichen und hinreichenden Bedingungen dafür, daß $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar ist, bestehen darin, erstens, daß f auch der Grad von $\mathfrak{p}$, also

$$N(\mathfrak{p}) = p^f, \tag{9}$$

und zweitens, daß $\mathfrak{p}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ ist.

In der Tat, wenn $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar ist, so ist $\mathfrak{o}$ der größte gemeinschaftliche Teiler dieser beiden Ideale und folglich auch derjenige von $\mathfrak{n}$ und $\mathfrak{p}$, weil $\mathfrak{k}$ durch $\mathfrak{n}$, und $\mathfrak{n}$ durch $\mathfrak{o}$ teilbar ist; hieraus folgt nach einem schon oft benutzten Satze (Z. § 165, S. 484)

$$(\mathfrak{n}, \mathfrak{p}) = (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}),$$

woraus sich mit Rücksicht auf (7) die zu beweisende Gleichung (9) ergibt. Ferner leuchtet ein, daß der größte gemeinschaftliche Teiler $\mathfrak{e}$ der Ideale $\mathfrak{o}p, \mathfrak{o}\varrho$ jedenfalls teilbar durch $\mathfrak{p}$ ist, weil zufolge (3) und (8) auch ϱ durch $\mathfrak{p}$ teilbar ist; daß aber wirklich $\mathfrak{e} = \mathfrak{p}$ ist, ergibt sich auf folgende Weise. Da $\mathfrak{k}\mathfrak{p}$ nicht durch $\mathfrak{p}^2$ teilbar ist, so gibt es in $\mathfrak{k}\mathfrak{p}$ eine durch $\mathfrak{p}^2$ nicht teilbare Zahl, welche gewiß von der Form $\psi(\theta)$ ist, weil $\mathfrak{k}\mathfrak{p}$ durch $\mathfrak{k}$, also auch durch $\mathfrak{n}$ teilbar ist; da nun $\psi(\theta)$ durch $\mathfrak{k}\mathfrak{p}$, mithin auch durch $\mathfrak{p}$ teilbar ist, so ist zufolge (5′)

$$\psi(t) \equiv P(t)\,\psi_1(t) \pmod{p},$$

also

$$\psi(\theta) \equiv \varrho\,\psi_1(\theta) \pmod{p},$$

woraus sich ergibt, daß die Zahlen p, ϱ nicht beide durch $\mathfrak{p}^2$ teilbar sein können, weil $\psi(\theta)$ nicht durch $\mathfrak{p}^2$ teilbar ist; mithin kann auch $\mathfrak{e}$ nicht durch $\mathfrak{p}^2$ teilbar sein. Ist ferner $\mathfrak{q}$ irgend ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal, so gibt es in dem Ideal $\mathfrak{k}\mathfrak{q}$, weil es nicht durch $\mathfrak{p}$ teilbar ist, eine durch $\mathfrak{p}$ nicht teilbare Zahl, welche wieder von der Form $\psi(\theta)$ ist, weil $\mathfrak{k}\mathfrak{q}$ durch $\mathfrak{k}$, also auch durch $\mathfrak{n}$ teilbar ist; da $\psi(\theta)$ nicht durch $\mathfrak{p}$, also $\psi(t)$ nicht durch $P(t)$ teilbar ist (mod. p), so gilt die Kongruenz (4), aus welcher, weil p und die in $\mathfrak{k}\mathfrak{q}$ enthaltene Zahl $\psi(\theta)$ durch $\mathfrak{q}$ teilbar sind, die Kongruenz

$$\varrho\,\psi_2(\theta) \equiv 1 \pmod{\mathfrak{q}}$$

folgt; mithin kann ϱ nicht durch $\mathfrak{q}$, also $\mathfrak{e}$ nicht durch $\mathfrak{p}\mathfrak{q}$ teilbar sein. Hieraus folgt offenbar, daß das in p aufgehende Ideal $\mathfrak{e} = \mathfrak{p}$ ist, womit der erste Teil unseres Satzes bewiesen ist.

Wir wenden uns jetzt zu dem bei weitem schwierigeren zweiten Teile: Wenn erstens der Grad f der Primfunktion $P(t)$ zugleich der Grad des Primideals $\mathfrak{p}$, und wenn zweitens $\mathfrak{p}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ ist, so haben wir zu zeigen, daß $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar ist. Wir bezeichnen mit $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$ und setzen

$$\mathfrak{o}p = \mathfrak{a}\mathfrak{p}^e, \tag{10}$$

wo $\mathfrak{a}$ ein durch $\mathfrak{p}$ nicht teilbares Ideal bedeutet, und wir wollen auf Grund unserer zweiten Annahme zunächst beweisen, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}^e} \tag{11}$$

mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p,\ P(t)^e} \tag{11'}$$

durchaus gleichbedeutend ist; in der Tat leuchtet unmittelbar ein, daß (11) eine Folge von (11') ist; findet aber (11') nicht statt, so ist der größte gemeinschaftliche Teiler, welchen $\psi(t)$ und $P(t)^e$ nach dem Modul p besitzen, von der Form $P(t)^r$, wo $r < e$ ist, und es gilt bekanntlich (K. § 4) eine Kongruenz von der Form

$$\psi(t)\,\psi_1(t) + P(t)^e\,\psi_2(t) \equiv P(t)^r \pmod{p},$$

aus welcher

$$\psi(\theta)\,\psi_1(\theta) \equiv \varrho^r \pmod{\mathfrak{p}^e}$$

folgt; im Falle $e = 1$ (der eigentlich schon oben in (5) und (5') erledigt ist) muß $r = 0$ sein, und folglich kann auch (11) nicht stattfinden; ist aber $e > 1$, also p teilbar durch $\mathfrak{p}^2$, so ist zufolge

unserer zweiten Annahme ϱ nicht teilbar durch $\mathfrak{p}^2$, mithin ist $\mathfrak{p}^r$ die höchste in ϱ^r aufgehende Potenz von $\mathfrak{p}$, also ϱ^r nicht teilbar durch $\mathfrak{p}^e$, und folglich kann auch in diesem Falle die Kongruenz (11) nicht stattfinden, was zu zeigen war. Aus dieser Äquivalenz zwischen (11) und (11′) folgt unmittelbar, daß die Anzahl der nach $\mathfrak{p}^e$ inkongruenten Zahlen von der Form $\psi(\theta)$ zugleich die Anzahl der nach dem Doppelmodul $p, P(t)^e$ inkongruenten Funktionen $\psi(t)$ ist, also (K. § 8)

$$(\mathfrak{n}, \mathfrak{p}^e) = p^{ef}.$$

Verbinden wir hiermit unsere erste Annahme (9), so ergibt sich

$$(12) \qquad (\mathfrak{n}, \mathfrak{p}^e) = N(\mathfrak{p}^e) = (\mathfrak{o}, \mathfrak{p}^e),$$

woraus wir schließen, daß $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{n}$ und $\mathfrak{p}^e$ ist, und daß alle Zahlklassen in bezug auf $\mathfrak{p}^e$ auch durch Zahlen der Ordnung $\mathfrak{n}$ repräsentiert werden können; ist daher ω eine beliebige Zahl in $\mathfrak{o}$, so gibt es immer eine Zahl ν in $\mathfrak{n}$, welche der Bedingung

$$(13) \qquad \omega \equiv \nu \pmod{\mathfrak{p}^e}$$

genügt. Wir ersetzen nun die Kongruenz (1) durch die folgende:

$$(14) \qquad F(t) \equiv A(t) P(t)^m \pmod{p},$$

wo $A(t)$ nach dem Modul p nicht durch $P(t)$ teilbar, also $m \geqq 1$ ist; dann ist zufolge (5) und (5′) die in $\mathfrak{n}$ enthaltene Zahl

$$(15) \qquad \alpha = A(\theta)$$

nicht teilbar durch $\mathfrak{p}$; da ferner $F(\theta) = 0$, mithin

$$(16) \qquad \alpha \varrho^m \equiv 0 \pmod{\mathfrak{a}\mathfrak{p}^e}$$

ist, so folgt

$$(17) \qquad \alpha \equiv 0 \pmod{\mathfrak{a}},$$

weil nach unserer zweiten Annahme ϱ relative Primzahl zu $\mathfrak{a}$ ist. Multipliziert man daher die Kongruenz (13) mit α, so erhält man

$$\omega\alpha \equiv \nu\alpha \pmod{p},$$

also

$$\omega\alpha = \nu\alpha + p\omega_1,$$

wo ω_1 eine ganze Zahl; da aber ν und α, mithin auch $\nu\alpha$ in der Ordnung $\mathfrak{n}$ enthalten ist, so folgt hieraus

$$(18) \qquad \omega\alpha \equiv p\omega_1 \pmod{\mathfrak{n}}.$$

Auf diese Weise kann man aus einer beliebig gewählten ganzen Zahl ω eine Kette von ganzen Zahlen $\omega, \omega_1, \omega_2 \cdots$ bilden, indem man

immer $\alpha\omega_r \equiv p\omega_{r+1} \pmod{\mathfrak{n}}$ setzt; da nun jede auf den Modul $\mathfrak{n}$ bezügliche Kongruenz mit jeder in $\mathfrak{n}$ enthaltenen Zahl, also mit p und α multipliziert werden darf, weil $\mathfrak{n}$ eine Ordnung ist, so ergibt sich allgemein, daß

$$\omega\alpha^r \equiv \omega_r p^r \pmod{\mathfrak{n}} \tag{19}$$

ist. Da nun θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades ist, so kann ihr Index k nicht verschwinden, und folglich kann man

$$k = (\mathfrak{o}, \mathfrak{n}) = hp^s \tag{20}$$

setzen, wo h eine durch p nicht teilbare ganze rationale Zahl bedeutet; setzen wir daher

$$\varkappa = h\alpha^s, \tag{21}$$

so ist $\varkappa$ nicht teilbar durch $\mathfrak{p}$, und da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{n}$ teilbar ist, so folgt aus (19) und (20)

$$\omega\varkappa \equiv k\omega_s \equiv 0 \pmod{\mathfrak{n}}. \tag{22}$$

Mithin wird jede ganze Zahl ω durch Multiplikation mit $\varkappa$ in eine Zahl der Ordnung $\mathfrak{n}$ verwandelt, d. h. das durch $\mathfrak{p}$ nicht teilbare Ideal $\mathfrak{o}\varkappa$ ist teilbar durch $\mathfrak{n}$; da nun der Führer $\mathfrak{f}$ einer Ordnung $\mathfrak{n}$ in jedem durch $\mathfrak{n}$ teilbaren Ideal aufgeht (§ 7), so ist $\mathfrak{f}$ nicht teilbar durch $\mathfrak{p}$, w. z. b. w.

§ 12.

Nachdem soeben die Bedingungen genau festgestellt sind, unter welchen der Führer einer regulären Ordnung durch ein gegebenes Primideal nicht teilbar ist, wollen wir beweisen, daß diese Bedingungen stets erfüllbar sind, d. h. daß folgender Satz besteht:

Ist $\mathfrak{p}$ ein gegebenes Primideal, so gibt es immer eine reguläre Ordnung $\mathfrak{n}$, deren Führer $\mathfrak{f}$ durch $\mathfrak{p}$ nicht teilbar ist.

In der Tat, wenn p die durch $\mathfrak{p}$ teilbare rationale Primzahl, und f der Grad von $\mathfrak{p}$, also

$$N(\mathfrak{p}) = p^f$$

ist, so wählen wir (wie in § 5, 5. oder in G. § 4) nach Belieben eine Funktion $P(t)$ von demselben Grade f, welche eine Primfunktion in bezug auf den Modul p ist, und unterwerfen die zu suchende Zahl θ, welche die reguläre Ordnung $\mathfrak{n}$ erzeugen soll, zunächst der Bedingung

$$P(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

welche Kongruenz bekanntlich immer f Wurzeln besitzt. Für den Fall, daß p durch $\mathfrak{p}^2$ teilbar ist, stellen wir ferner an θ die Forderung, daß $P(\theta)$ nicht durch $\mathfrak{p}^2$ teilbar ist, was sich ebenfalls erreichen läßt, weil die Derivierte $P'(t)$ in bezug auf p relative Primfunktion zu $P(t)$ ist (G. § 4). Ist ferner $\mathfrak{q}$ irgend ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal, so gibt es jedenfalls Zahlen μ, für welche $P(\mu)$ nicht durch $\mathfrak{q}$ teilbar ist; denn wenn etwa die rationale Zahl $P(0)$ durch $\mathfrak{q}$ und folglich auch durch p teilbar ist, was nur dann geschieht, wenn $P(t) \equiv t \pmod{p}$, so ist $P(1)$ nicht teilbar durch $\mathfrak{q}$, mithin ist mindestens eine der beiden Zahlen 0, 1 eine solche Zahl μ. Wählt man nun die Zahl θ so, daß sie in bezug auf jedes Primideal $\mathfrak{q}$ einer entsprechenden solchen Zahl μ kongruent wird, welche Bedingungen bekanntlich untereinander und auch mit der früheren, auf $\mathfrak{p}$ oder $\mathfrak{p}^2$ bezüglichen verträglich sind, so wird offenbar $\mathfrak{p}$ der größte gemeinschaftliche Teiler von p und $P(\theta)$, und dies bleibt auch bestehen, wenn θ durch irgend eine andere Zahl derselben Zahlklasse (mod. p) ersetzt wird. Die beiden in dem Satze des vorigen Paragraphen aufgestellten charakteristischen Bedingungen sind dann immer erfüllt, und wir haben daher nur noch zu zeigen, daß aus einer solchen Zahlklasse, welche den bisherigen Bedingungen genügt, die Zahl θ immer so ausgewählt werden kann, daß die abgeleitete Zahl θ^* nicht verschwindet, daß also θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades wird und folglich eine wirkliche Ordnung $\mathfrak{n}$ erzeugt, welche dann unfehlbar die verlangte Eigenschaft besitzen muß. Hierzu gelangt man leicht auf folgende Weise. Da jeder Körper n^{ten} Grades Ω gewiß Zahlen enthält, die einer irreduktibelen Gleichung n^{ten} Grades genügen*), so gibt es unter ihnen auch ganze Zahlen, und es sei ω eine solche; setzen wir wieder fest (wie in § 1), daß die Permutation $\varphi^{(1)}$ alle Zahlen ungeändert läßt, so ist

$$\omega^* = (\omega - \omega^{(2)})(\omega - \omega^{(3)}) \cdots (\omega - \omega^{(n)})$$

und ebenso

$$\theta^* = (\theta - \theta^{(2)})(\theta - \theta^{(3)}) \cdots (\theta - \theta^{(n)}).$$

Ist nun ξ eine bestimmte Zahl, welche allen der Zahl θ oben auferlegten Kongruenzbedingungen genügt, und setzt man

$$\theta = \xi + p x \omega,$$

*) Dies liegt entweder schon in der Definition von Ω (Z. S. 464, 469), oder es wird leicht bewiesen, falls diese Definition durch eine andere ersetzt wird (zweite Auflage der Zahlentheorie, S. 425, 427).

wo x eine willkürliche ganze rationale Zahl bedeutet, so genügt auch diese Zahl θ denselben Bedingungen; da ferner ω^* von Null verschieden ist, so gilt dasselbe von den $(n-1)$ Differenzen $\omega - \omega^{(r)}$, wo r die Werte $2, 3 \cdots n$ durchläuft, und man kann folglich die Zahl x immer so wählen, daß keine der Differenzen

$$\theta - \theta^{(r)} = (\xi - \xi^{(r)}) + p\,x\,(\omega - \omega^{(r)})$$

verschwindet, mithin auch deren Produkt θ^* von Null verschieden wird, w. z. b. w.

Dem Beweise des Satzes wollen wir, um etwaigen Mißverständnissen vorzubeugen, noch folgende Bemerkung hinzufügen. Wenn ein Primideal $\mathfrak{p}$ gegeben ist, so kann man, wie eben bewiesen ist, immer eine reguläre Ordnung konstruieren, deren Führer durch $\mathfrak{p}$ nicht teilbar ist. Sind aber zwei verschiedene Primideale $\mathfrak{p}$, $\mathfrak{q}$ gegeben, so kann schon der Fall eintreten, daß jeder Führer einer regulären Ordnung durch mindestens eins der Ideale $\mathfrak{p}$, $\mathfrak{q}$ teilbar ist. Ein einfaches Beispiel hierfür liefert der in der früheren Abhandlung (G. § 5) betrachtete kubische Körper Ω, dessen Grundzahl $D = -503$ ist*); es ist dort gezeigt, daß der Index k einer jeden ganzen Zahl θ eine gerade Zahl, und daß $\mathfrak{o}(2) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$ ist, wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ voneinander verschiedene Primideale ersten Grades bedeuten; und dies reicht hin, um unsere Behauptung mit Zuziehung der jetzigen allgemeinen Theorie zu rechtfertigen. Ist nämlich θ eine bestimmte Zahl und 2^s die höchste in ihrem Index k aufgehende Potenz von 2, so ist $s > 0$, und wenn man mit $\mathfrak{a}^a$, $\mathfrak{b}^b$, $\mathfrak{c}^c$ die höchsten Potenzen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ bezeichnet, welche in dem entsprechenden Ordnungsführer $\mathfrak{f}$ aufgehen, so sind die Exponenten a, b, c alle $\leqq s$, weil k immer durch $\mathfrak{f}$ teilbar ist; da ferner $N(\mathfrak{a}) = N(\mathfrak{b}) = N(\mathfrak{c}) = 2$ und $N(\mathfrak{f}) = k^2$ ist (§ 9, (16)), so ist 2^{a+b+c} die höchste in k^2 aufgehende Potenz von 2, folglich $a + b + c = 2s$; mithin kann von den drei Exponenten a, b, c, weil sie $\leqq s$ sind, höchstens einer $= 0$ sein, d. h. $\mathfrak{f}$ ist teilbar durch mindestens zwei der drei Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ (also auch durch mindestens eins der beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$). Diese theoretischen Vorhersagungen bestätigen sich vollständig durch die wirkliche Rechnung, und man findet z. B. leicht, daß $\mathfrak{a}\mathfrak{c}$, $\mathfrak{b}\mathfrak{c}$, $\mathfrak{a}\mathfrak{b}$ die Führer der regulären Ordnungen sind, welche durch die dort mit α, β, $\alpha + \beta$ bezeichneten Zahlen erzeugt werden.

*) Daß zu dieser Grundzahl nur ein einziger kubischer Körper oder vielmehr drei konjugierte Körper gehören, hängt mit tieferen Gesetzen zusammen, welche den Gegenstand einer anderen Abhandlung bilden sollen.

§ 13.

Der im vorigen Paragraphen bewiesene Satz kann mit Rücksicht auf den Satz (11) in § 10 folgendermaßen ausgesprochen werden:

Das Grundideal $\mathfrak{d}$ ist der größte gemeinschaftliche Teiler aller Zahlen $\theta^* = F'(\theta)$, welche allen ganzen Zahlen θ des Körpers entsprechen.

Wir stützen uns nun auf die gewonnenen Resultate, um die Konstitution des Grundideals $\mathfrak{d}$ zu erforschen, d. h. um zu untersuchen, ob und wie oft ein gegebenes Primideal $\mathfrak{p}$ als Faktor von $\mathfrak{d}$ auftritt. Zu diesem Zweck wählen wir die ganze Zahl θ so, daß der Führer $\mathfrak{k}$ der durch sie erzeugten regulären Ordnung $\mathfrak{n}$ nicht durch $\mathfrak{p}$ teilbar ist, und behalten alle in den letzten Paragraphen gebrauchten Bezeichnungen bei. Wir wollen jetzt zeigen, daß die beiden durch die Gleichung (10) und die Kongruenz (14) in § 11 definierten Exponenten e und m einander gleich sind. In der Tat, da die Zahl α nicht durch $\mathfrak{p}$ teilbar ist, so folgt aus der dortigen Kongruenz (16)

$$\varrho^m \equiv 0 \pmod{\mathfrak{p}^e},$$

und hieraus zunächst $m \geqq e$; dies leuchtet unmittelbar ein, wenn $e = 1$ ist; wenn aber $e > 1$, also p durch $\mathfrak{p}^2$ teilbar ist, so kann, wie damals bewiesen ist, ϱ nicht durch $\mathfrak{p}^2$ teilbar sein, mithin ist $\mathfrak{p}^m$ die höchste in ϱ^m aufgehende Potenz von $\mathfrak{p}$, woraus unsere Behauptung folgt. Umgekehrt, da zufolge der dortigen Kongruenz (17) die Zahl α durch das Ideal $\mathfrak{a}$, ferner ϱ durch $\mathfrak{p}$ teilbar ist, so kann man zufolge der dortigen Gleichung (10)

$$\alpha \varrho^e = p\omega$$

setzen, wo ω eine ganze Zahl bedeutet; multipliziert man mit der durch die dortige Gleichung (21) definierten Zahl $\varkappa = h\alpha^s$, so erhält man

$$h\alpha^{s+1}\varrho^e = p\varkappa\omega;$$

nun ist damals in (22) gezeigt, daß $\varkappa\omega$ in $\mathfrak{n}$ enthalten, also eine Zahl von der Form $\psi(\theta)$ ist; die vorstehende Gleichung geht daher, wenn wir noch α und ϱ durch ihre Ausdrücke $A(\theta)$ und $P(\theta)$ ersetzen, in die folgende über:

$$hA(\theta)^{s+1}P(\theta)^e = p\psi(\theta).$$

Hieraus folgt wegen der Irreduktibilität der Gleichung $F(\theta) = 0$ eine Identität von der Form

$$hA(t)^{s+1}P(t)^e = p\psi(t) + F(t)\psi_1(t),$$

und da m durch die Kongruenz

$$F(t) \equiv A(t)\,P(t)^m \pmod{p}$$

definiert war, so erhalten wir

$$h\,A(t)^{s+1}\,P(t)^e \equiv A(t)\,\psi_1(t)\,P(t)^m \pmod{p}$$

oder auch

$$h\,A(t)^s\,P(t)^e \equiv \psi_1(t)\,P(t)^m \pmod{p}.$$

Da nun die rationale Zahl h nicht durch p teilbar, und die Funktion $A(t)$ nicht durch die Primfunktion $P(t)$ teilbar ist (mod. p), so ist $P(t)^e$ die höchste in der linken Seite aufgehende Potenz von $P(t)$, und da die rechte Seite durch $P(t)^m$ teilbar ist, so muß nach dem Fundamentalsatze (K. § 6) in der Theorie der höherer Kongruenzen $e \geqq m$ sein. Oben haben wir aber schon bewiesen, daß $m \geqq e$ ist, und wir erhalten folglich das Resultat

(1) $$m = e,$$

wo e (zufolge § 11, (10)) den Exponenten der höchsten in p aufgehenden Potenz von $\mathfrak{p}$ bedeutet. Zugleich ist also

(2) $$F(t) \equiv A(t)\,P(t)^e \pmod{p},$$

d. h.

$$F(t) = A(t)\,P(t)^e - p\,M(t),$$

und wir wollen beiläufig bemerken, daß, wenn $e > 1$ ist, die hier auftretende Funktion $M(t)$ nach dem Modul p nicht durch $P(t)$ teilbar sein kann; denn $P(\theta)$ ist in diesem Falle (zufolge § 11) nicht teilbar durch $\mathfrak{p}^2$, und folglich ist $\mathfrak{p}^e$ die höchste Potenz von $\mathfrak{p}$, welche in der linken Seite der Gleichung

$$A(\theta)\,P(\theta)^e = p\,M(\theta)$$

aufgeht, und da $\mathfrak{p}^e$ auch in p aufgeht, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein, woraus unsere Behauptung folgt, welche von Interesse für die in der früheren Abhandlung (G. § 3) ausgeführte Untersuchung der Funktion $M(t)$ ist.

Durch Differentiation der Kongruenz (2) ergibt sich nun, wenn wir zur Abkürzung

(3) $$B(t) = P(t)\,A'(t) + e\,A(t)\,P'(t)$$

setzen, die folgende Kongruenz:

(4) $$F'(t) \equiv B(t)\,P(t)^{e-1} \pmod{p},$$

aus welcher zunächst

(5) $$\theta^* \equiv B(\theta)\,P(\theta)^{e-1} \pmod{p},$$

also jedenfalls

(6) $$\theta^* \equiv 0 \pmod{\mathfrak{p}^{e-1}}$$

folgt. Um aber zu entscheiden, ob $\mathfrak{p}^{e-1}$ die höchste in θ^* aufgehende Potenz von $\mathfrak{p}$ ist, müssen wir zwei wesentlich verschiedene Fälle unterscheiden. Erstens, wenn der Exponent e nicht teilbar durch p ist, so geht aus (3) hervor, daß die Funktion $B(t)$ nach dem Modul p nicht durch $P(t)$ teilbar ist, weil dasselbe auch von $A(t)$ und $P'(t)$ gilt; mithin ergibt sich aus (4), daß $F'(t)$ nach dem Modul p nicht durch $P(t)^e$ teilbar ist, und hieraus folgt nach einem früheren Satze (§ 11, (11) und (11')), daß die Zahl $F'(\theta)$ nicht durch $\mathfrak{p}^e$ teilbar ist; mithin ist in diesem Falle $\mathfrak{p}^{e-1}$ die höchste in der Zahl θ^* aufgehende Potenz von $\mathfrak{p}$. Zweitens, wenn der Exponent e teilbar durch p ist, so ist die Funktion $B(t)$ offenbar durch $P(t)$, mithin $F'(t)$ durch $P(t)^e$ teilbar (mod. p), woraus sich ergibt, daß in diesem Falle die Zahl θ^* mindestens durch $\mathfrak{p}^e$, vielleicht aber auch durch noch höhere Potenzen von $\mathfrak{p}$ teilbar ist.

Da nun der Führer $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar, und (zufolge § 10, (11))

$$\mathfrak{o}\theta^* = \mathfrak{d}\mathfrak{k}$$

ist, so sind die Ideale $\mathfrak{o}\theta^*$ und $\mathfrak{d}$ durch gleich hohe Potenzen von $\mathfrak{p}$ teilbar, und somit erhalten wir den folgenden Fundamentalsatz:

Ist $\mathfrak{p}$ ein beliebiges Primideal, p die durch $\mathfrak{p}$ teilbare rationale Primzahl, und $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$, so ist das Grundideal $\mathfrak{d}$ allemal teilbar durch $\mathfrak{p}^{e-1}$; ist ferner der Exponent e nicht teilbar durch p, so ist $\mathfrak{d}$ nicht teilbar durch $\mathfrak{p}^e$; ist aber e teilbar durch p, so ist $\mathfrak{d}$ teilbar durch $\mathfrak{p}^e$ und vielleicht durch noch höhere Potenzen von $\mathfrak{p}$.

§ 14.

Man erkennt leicht, daß der Satz über die Teilbarkeit der Grundzahl D durch eine Primzahl p, von welchem wir in § 3 einen unvollständigen, in den folgenden §§ 4 — 6 aber einen vollständigen Beweis gegeben haben, jetzt aus der Verbindung des eben gewonnenen Resultates über das Grundideal $\mathfrak{d}$ mit dem Satze $N(\mathfrak{d}) = (D)$ unmittelbar hervorgehen muß. In der Tat, wenn die rationale Primzahl p durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar ist, so geht $\mathfrak{p}$ jedenfalls in dem Grundideal $\mathfrak{d}$ auf, dessen Norm (D) mithin durch $N(\mathfrak{p})$, also auch durch p teilbar ist. Umgekehrt, wenn D, also auch $N(\mathfrak{d})$ durch p teilbar ist, so muß nach einem bekannten Satze

(Z. § 174, 8.) das Ideal $\mathfrak{d}$ selbst durch ein in p aufgehendes Primideal $\mathfrak{p}$ teilbar sein, und folglich muß $\mathfrak{p}^2$ in p aufgehen, w. z. b. w.

Aber es leuchtet ein, daß wir durch diesen Satz über das Grundideal $\mathfrak{d}$ eine viel tiefere Grundlage gewonnen haben, insofern derselbe die Konstitution dieses Ideals und folglich auch diejenige der Grundzahl D — von gewissen singulären Fällen abgesehen — genau bestimmt. Ein solcher Ausnahmefall tritt nur dann ein, wenn der Exponent e der höchsten in p aufgehenden Potenz von $\mathfrak{p}$ selbst durch p teilbar ist, und da e niemals größer als der Grad n des Körpers sein kann, weil die Norm von $\mathfrak{p}^e$ in p^n aufgeht, so können von der in unserem Satze enthaltenen Unbestimmtheit höchstens solche Primzahlen p getroffen werden, die $\leqq n$ sind. Diese Unbestimmtheit ist auch in der Natur der Sache selbst begründet und nicht etwa einem Mangel in unserer Untersuchung zuzuschreiben; es wird wenigstens nicht leicht sein, diese Ausnahmefälle doch auf bestimmte einfache Gesetze zurückzuführen. In der Tat, wenn der Exponent e durch p teilbar ist, und wenn man mit r den Exponenten der höchsten in $\mathfrak{d}$ aufgehenden Potenz von $\mathfrak{p}$ bezeichnet, so kann es geschehen, daß $r = e$ ist, aber es kann auch $r > e$ sein, ja man kann sogar, wenn irgend ein Vielfaches von e gegeben ist, Fälle nachweisen, in denen r dieses Vielfache überschreitet. Um die große Mannigfaltigkeit der hierbei auftretenden Erscheinungen darzutun, wollen wir nur zwei Beispiele anführen.

Ist Ω ein quadratischer Körper, also $n = 2$, und p eine in der Grundzahl D aufgehende Primzahl, so ist p durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar, und hieraus folgt mit Notwendigkeit, daß

$$\mathfrak{o}\,p = \mathfrak{p}^2, \quad e = 2, \quad N(\mathfrak{p}) = p, \quad f = 1$$

ist, weil allgemein die Anzahl der Primideale, deren Produkt $= \mathfrak{o}\,p$ ist, niemals größer als der Grad n des Körpers Ω sein kann. Ist nun p ungerade, also der Exponent e nicht teilbar durch p, so ist das Grundideal $\mathfrak{d}$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar, und folglich ist dessen Norm (D) durch p, aber nicht durch p^2 teilbar. Ist aber $p = 2$, also der Exponent e teilbar durch p, so ist $\mathfrak{d}$ mindestens durch $\mathfrak{p}^2$, und folglich D mindestens durch 4 teilbar, und es sind zwei Fälle möglich: die höchste in $\mathfrak{d}$ aufgehende Potenz von $\mathfrak{p}$ ist $= \mathfrak{p}^2$ oder $= \mathfrak{p}^3$, je nachdem $\frac{1}{4}D \equiv 3$ oder $\equiv 2 \pmod 4$ ist. In allen Fällen ist

$$\mathfrak{o}\,D = \mathfrak{d}^2, \quad \mathfrak{o}\sqrt{D} = \mathfrak{d}.$$

Wir wollen zweitens den Kreisteilungskörper Ω betrachten, welcher aus einer primitiven Wurzel θ der Gleichung $\theta^m = 1$ entspringt, und dessen Grad $n = \varphi(m)$ ist. Man findet ohne erhebliche Schwierigkeit, daß auch in diesem Falle das Gebiet $\mathfrak{o}$ selbst eine reguläre Ordnung, nämlich

$$\mathfrak{o} = [1, \theta, \theta^2 \cdots \theta^{n-1}],$$

und folglich das Grundideal $\mathfrak{d} = \mathfrak{o}\theta^*$ ist; die Grundzahl D ergibt sich (wenn $m > 2$ ist) aus der Gleichung

$$D \Pi p^{\frac{n}{p-1}} = (-1)^{\frac{1}{2}n} m^n,$$

wo das Produktzeichen Π sich auf alle in m aufgehenden Primzahlen p bezieht. Setzt man ferner

$$m = m' p^s, \quad \varphi(p^s) = e,$$

wo m' nicht teilbar durch p, und bedeutet f den kleinsten positiven Exponenten, für welchen

$$p^f \equiv 1 \pmod{m'}$$

ist, so ist

$$\varphi(m') = af, \quad n = aef,$$

und man findet, daß

$$\mathfrak{o}p = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_a)^e$$

ist, wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_a$ voneinander verschiedene Primideale vom Grade f sind. Diese Zerlegung gilt für jede Primzahl p, auch wenn sie in m nicht aufgeht und folglich durch kein Primideal-Quadrat teilbar ist ($s = 0$, $e = 1$); uns interessiert aber nur der entgegengesetzte Fall $s > 0$, und dann ist

$$\mathfrak{o}(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_a.$$

Bezeichnen wir mit $\mathfrak{p}$ irgend eins dieser Primideale, so hat die höchste in p aufgehende Potenz von $\mathfrak{p}$ den Exponenten

$$e = (p-1)p^{s-1};$$

bezeichnet man ferner mit r den Exponenten der höchsten in dem Grundideal $\mathfrak{d}$ aufgehenden Potenz von $\mathfrak{p}$, so ist

$$\mathfrak{d} = \mathfrak{a}(1 - \theta^{m'})^r,$$

wo $\mathfrak{a}$ relatives Primideal zu p ist und

$$r = se - \frac{e}{p-1} = (s(p-1) - 1)p^{s-1}.$$

Der Exponent e ist nur dann nicht durch p teilbar, und zwar $= p-1$, wenn $s = 1$, also m nicht teilbar durch p^2 ist, und zugleich ist der

Exponent $r = e - 1 = p - 2$; ist aber m teilbar durch p^2, also $s \geqq 2$, so ist e teilbar durch p, und zugleich $r > e$, ausgenommen den Fall $p = 2$, $s = 2$, in welchem $r = e = 2$ ist.

Da man m so wählen kann, daß s beliebig groß ist, so wird hierdurch unsere obige Behauptung gerechtfertigt, daß es Beispiele gibt, in welchen der Exponent r ein beliebiges, gegebenes Vielfaches $(s-1)e$ des Exponenten e überschreitet. Achtet man aber zugleich auf die höchste in e selbst aufgehende Potenz von p (welche in unserem Beispiele $= p^{s-1}$ ist), so scheint es allerdings, als ob sich eine obere Grenze für r angeben lasse, und vielleicht gilt für beliebige Körper der Satz, daß stets $r < se$ ist, wenn $s-1$ der Exponent der höchsten in e aufgehenden Potenz von p ist. Indessen wage ich hierüber keine Vermutung zu äußern, nachdem einige flüchtige Versuche, zu einem Beweise zu gelangen, mir mißglückt sind.

Erläuterungen zur vorstehenden Abhandlung.

In dieser klassisch gewordenen Abhandlung gibt Dedekind zum ersten Male die Grundlage der allgemeinen Verzweigungstheorie in algebraischen Körpern; die große Tragweite der rein arithmetischen Methoden von Dedekind tritt bei der Behandlung dieser Probleme besonders klar hervor.

Die Verzweigungstheorie in der Kroneckerschen Formentheorie (Journ. f. Math., Bd. 92, S. 1—122 (1882)) ist von Hensel (ebenda, Bd. 113, S. 61—83 (1894)) entwickelt worden; unter Anwendung einer etwas anderen Definition der Differente $\mathfrak{d}$ (= Grundideal von Dedekind) erhält man hierin einen einfachen Beweis des ersten Dedekindschen Hauptsatzes

$$|D| = N(\mathfrak{d}). \tag{1}$$

In der Henselschen Theorie der p-adischen Zahlen (Hensel, Theorie der algebraischen Zahlen I, Leipzig 1908) werden außer der Kroneckerschen Theorie auch noch arithmetische Methoden angewandt, welche prinzipiell mit den Dedekindschen eine gewisse Ähnlichkeit zeigen.

Weitere Beweise von (1) und dem zweiten Dedekindschen Hauptsatze

$$f'(\theta) = \mathfrak{f} \cdot \mathfrak{d} \qquad (\mathfrak{f} = \text{Führer})$$

findet man bei Hilbert (Jahresber. d. Deutsch. Math. Vereinigung, Bd. 4 (1894)), Landsberg (Gött. Nachr. 1897, S. 277—303), Bauer (Acta litt. ac. scient. reg. univ. Hungaricae, Bd. 1, S. 195—198 (1923), Math. Zeitschr., Bd. 16, S. 1—12 (1923)). Eine besonders einfache Beweisanordnung gibt Hecke (Vorlesungen über die Theorie der algebraischen Zahlen, § 36, Leipzig 1923).

Auf die in der Einleitung versprochenen Behandlung der Verzweigungstheorie in Relativkörpern, ist Dedekind nicht zurückgekommen. Die wichtigsten Resultate auf diesem Gebiete verdankt man Hilbert (l. c. Kap. V). Die eben erwähnte Methode von Hecke läßt sich auch unmittelbar auf Relativkörper verallgemeinern (Hecke, l. c. § 38).

Eine Übertragung des Dedekindschen Diskriminantensatzes auf Ringe (Ordnungen) in (endlichen) algebraischen Körpern gab E. Noether (Journ. f. Math., Bd. 157, S. 82—104 (1927)); für die Verzweigungstheorie in Ringen vgl. die in dieser Abhandlung angegebene Literatur.

In der Fußnote am Ende des § 7 gibt Dedekind die notwendige und hinreichende Bedingung dafür, daß ein Ideal Führer eines Ringes (Ordnung) ist. Furtwängler (Sitzungsber. Wien, Abt. IIa, Bd. 128, S. 239—245 (1920)) hat, wahrscheinlich ohne die Dedekindsche Fußnote bemerkt zu haben, ein weiteres Kriterium angegeben, das aber, wie man leicht sieht, mit dem Dedekindschen äquivalent ist (vgl. auch Referat in den Fortschritten d. Math., Bd. 47, S. 146). Die Eigenschaften der Führer der regulären Ringe

$$\mathfrak{n} = [1, \theta, \ldots, \theta^{n-1}]$$

sind von Ore (Math. Ann., Bd. 96, S. 313—352 (1926)) studiert worden.

In seiner Schlußbemerkung spricht Dedekind die Vermutung aus, daß im singulären Falle, wenn die Ordnungszahl e eines Primideals $\mathfrak{p}$ genau durch p^s, $s \geqq 1$ teilbar ist, die Differente genau durch eine Potenz $\mathfrak{p}^\varkappa$ teilbar wird, wo

$$e \leqq \varkappa < (s+1)e \tag{2}$$

gilt. Diese Vermutung wurde zuerst von Hensel (Gött. Nachr. 1897, S. 247—253, Math. Ann., Bd. 55, S. 301—336 (1902)) bewiesen. Weitere Beweise gaben Bauer (Math. Ann., Bd. 83, S. 74—76 (1921)) und Ore (Math. Ann., Bd. 96, S. 313—352 (1926)). Ore (l. c.) hat auch gezeigt, daß zwischen den beiden Grenzen in (2) gewisse Ausnahmewerte vorkommen, welche $\varkappa$ nie annehmen kann, während alle übrigen, nach (2) möglichen Werte von $\varkappa$ auch in passend gewählten Körpern realisiert werden können. (Spezialfälle in den obenerwähnten Arbeiten von Bauer.) Hieraus folgt weiter für ein gegebenes n und p die genaue obere Grenze für die höchste Potenz von p, welche in der Diskriminante eines Körpers n-ten Grades vorkommen kann. Auch hier sind alle möglichen Exponenten bestimmbar. (Spezialfall bei Stickelberger (Intern. Math. Kongreß, Zürich 1897, S. 182—193).) Die Verallgemeinerung der Dedekind-Henselschen Ungleichung (2) auf Relativkörper gab Ore (Math. Ann., Bd. 97, S. 569—598 (1927)).

Für die Körperdiskriminante besteht der bekannte Satz von Minkowski: $|D| > 1$ (Verh. d. Naturf. zu Bremen 1890, Geometrie der Zahlen 1896; weitere Literatur vgl. Dickson, Mitchell, Vandiver, Wahlin, Algebraic numbers § 29. Bulletin of the National Research Council, Vol. 5, no. 28 (1923)).

Ore.